User Manual

Allen-Bradley

Stratix 5700 Ethernet Managed Switches

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

	WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

	SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
	ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

Allen-Bradley, ArmorStratix 5700, Logix5000, Rockwell Automation, Rockwell Software, RSLinx, RSLogix, RSNetWorx, Stratix 2000, Stratix 5700, Stratix 8000, Stratix 8300, Studio 5000, Studio 5000 Automation Engineering & Design Environment, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

New and Updated Information

This table contains the changes made to this revision.

Topic	Page
New switch catalog number descriptions	16
New switch dimensions	18, 21
100BASE-FX/SX and 1000BASE-FX/SX port descriptions	23
ArmorStratix 5700 switch installation	57…66
Express Setup on SFP-port switches	67, 68, 70, 73
Power over Ethernet (PoE) configuration in Studio 5000 environment	201
Module-defined data types for 8-, 16-, and 24-port switches	247, 248, 252, 254, 267, 270
CIP data assignments for 8-, 16-, and 24-port switches	271
ArmorStratix 5700 console port	278

Notes:

Preface

Studio 5000 Environment 11
Access Product Release Notes 12
Additional Resources 13

Chapter 1

About the Switches

Switch Catalog Numbers 16
Switch Software Features 17
Stratix 5700 Switch Dimensions 18
ArmorStratix 5700 Switch Dimensions 21
Switch Front Panel 22
Switch Hardware Features 22
Configuration Files 23
SD Card 23
SD Card Sync 24
Switch Memory Allocation 25
Device Manager Web Interface 26
Hardware Requirements 26
Software Requirements 26
Studio 5000 Environment 27
Hardware Requirements 27
Cisco Network Assistant 27
Command Line Interface 28

Chapter 2

Switch Installation

Stratix 5700 Switch Installation 30
Installation Guidelines 31
Install or Remove the SD Card (optional) 33
Verify Switch Operation 34
Mount the Switch on a DIN Rail 36
Remove the Switch from the DIN Rail 38
Ground the Switch 38
Wire the Switch DC Power Source 40
Attach the Switch Power Connectors 43
Wire the Power over Ethernet DC Power Source 44
Attach the PoE Power Connector 46
Install an SFP Module (optional) 46
Remove SFP Modules from SFP Module Slots 48
Wire the External Alarms 49
Attach the Alarm Relay Connector to the Switch 52
Connect to 10/100 and 10/100/1000 Ports 52
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports 53
Connect to PoE Ports 54
Connect to SFP Modules 55
Connect to a Dual-purpose Port 56

ArmorStratix 5700 Switch Installation 57
Installation Guidelines 57
Install or Remove the SD Card (optional) 59
Verify Switch Operation 60
Mount the Switch 61
Ground the Switch 62
Connect the Switch to a DC Power Source 64
Wire External Alarms 65
Connect to 10/100 and 10/100/1000 Ports 66
Connect to PoE Ports 66
Set Up the Switch Initially with Express Setup 67

Chapter 3

Switch Software Features

Port Numbering 76
Global Macro 82
Smartports 83
Optimize Ports through Smartports Port Roles 83
Custom Smartport Roles 83
Avoid Smartport Mismatches 84
Power over Ethernet (PoE) 85
Powered Device Detection and Initial Power Allocation 86
Power Management Modes 87
VLANs 90
Isolate Traffic and Users 91
Isolate Different Traffic Types 92
Group Users 92
IGMP Snooping with Querier 93
Spanning Tree Protocol 94
Port Thresholds 95
Incoming (storm control) 95
Outgoing (rate limiting) 96
Default Port Thresholds Configuration 96
Port Security 97
Dynamic Secure MAC Address (MAC ID) 97
Static Secure MAC Address (MAC ID) 98
Security Violations 98
EtherChannels 98
DHCP Persistence 100
CIP Sync Time Synchronization (Precision Time Protocol) 100
Network Address Translation (NAT) 101
Configuration Overview 101
VLAN Assignments 105
Configuration Considerations 106
Traffic Permits and Fixups 106

Resilient Ethernet Protocol 107
REP Open Segment 108
REP Ring Segment 109
Access Ring Topologies 109
Link Integrity 110
SNMP 111
Supported MIBs. 112
Port Mirroring. 113
Routing 113
Configuration Management 114
SD Card Synchronization. 114
Alarms 114
Cryptographic IOS Software (optional) 114
Cable Diagnostics 115
Advanced Software Features 115

Chapter 4

Manage the Switch via the Device Manager Web Interface

Access the Device Manager Web Interface. 118
Dashboard Overview 119
Front Panel and Status Indicators 119
Switch Information. 122
Switch Health. 123
Port Utilization 124
Configure Smartports 125
Customize Port Role Attributes 126
Manage Custom Smartport Macros 127
Configure Port Settings. 132
Configure Port Thresholds 134
Configure EtherChannels. 135
Configure DHCP. 137
Set up the DHCP Server 137
Configure a DHCP IP Address Pool 138
Reserve IP Addresses through DHCP Persistence 139
Configure VLANs 141
Assign Ports to VLANs 142
Configure Power over Ethernet (PoE) Ports 142
Configure PTP Time Synchronization 145
Enable and Configure Routing 148
Enable Connected Routing Only 148
Enable Both Static and Connected Routing. 148
Configure STP. 149
Global Settings 149
PortFast Settings 150
Configure REP 151

Configure NAT 153
Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router 153
Create NAT Instances for Traffic Routed through a Layer 2 Switch 157
Configure Traffic Permits and Fixups 161
Configure Port Security 162
Configure IGMP Snooping 164
Configure SNMP 165
Use SNMP Management Applications 166
Configure Alarm Settings 166
Alarm Relay Settings 166
Global Alarms 167
Port Alarms 168
Configure Alarm Profiles 168
Monitor Trends 170
Monitor Port Statistics 171
Monitor NAT Statistics 172
Monitor REP Topology 173
Monitor CIP Status 174
Diagnose Cabling Problems 176
View System Log Messages 177
Use Express Setup to Change Switch Settings 178
Manage Users 180
Reallocate Switch Memory for Routing 181
Restart the Switch 182
Upgrade the Switch Firmware 183
Use the SD Card to Synchronize the Configuration or IOS Files 184
Upload and Download Configuration Files 186
Upgrade License Files 186

Chapter 5

Manage the Switch via the Studio 5000 Environment

EtherNet/IP CIP Interface 188
CIP Network Connections 188
RSLinx Software and Network Who Support 189
Electronic Data Sheet (EDS) Files 189
Data Accessible With CIP 190
Add a Switch to the I/O Configuration Tree 191
Configure General Properties 192
Connection Properties 195
Module Information 196
Switch Configuration Properties 197
Switch Status 199
Port Configuration 200
Power over Ethernet (PoE) 201
Smartports and VLANs 203
Port Thresholds 205

Port Security 206
Port Status 207
Port Diagnostics 208
Cable Diagnostics 209
DHCP Pool Display 210
DHCP Address Assignment 212
Time Sync Configuration 213
NAT Configuration 215
Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router 216
Create NAT Instances for Traffic Routed through a Layer 2 Switch 220
Configure Traffic Permits and Fixups 228
View Address Translations in RSLinx Software 229
NAT Diagnostics 229
Private-to-Public Translation Diagnostics 231
Public-to-Private Translation Diagnostics 232
SD Flash Sync 233
Save and Restore the Switch Configuration 234

Chapter 6

Troubleshoot the Switch

Verify Boot Fast 235
IP Address Issues 235
Device Manager Web Interface Issues 236
Switch Performance 237
Access Direct Managed Mode 237
Restart or Reset the Switch 239
Restart the Switch from the Device Manager Web Interface 239
Restart the Switch from the Logix Designer Application 239
Reset the Switch to Factory Defaults 240
Recover the Switch Firmware and Restore Factory Defaults 240
Troubleshoot a Firmware Upgrade 241

Appendix A

Module-defined Data Types

Module-defined Input Data Type (6-port Gb switches) 245
Module-defined Output Data Type (6-port Gb switches) 246
Module-defined Input Data Type (6-port switches) 246
Module-defined Output Data Type (6-port switches) 247
Module-defined Input Data Type (8-port switches) 247
Module-defined Output Data Type (8-port switches) 248
Module-defined Input Data Type (10-port Gb switches) 249
Module-defined Output Data Type (10-port Gb switches) 250
Module-defined Input Data Type (10-port switches) 250
Module-defined Output Data Type (10-port switches) 252
Module-defined Input Data Type (16-port switches) 252
Module-defined Output Data Type (16-port switches) 254

Module-defined Input Data Type (20-port Gb switches) 254
Module-defined Input Data Type (18-port Gb switches) 257
Module-defined Output Data Type (18-port Gb switches)..... 260
Module-defined Input Data Type (20-port Gb switches) 261
Module-defined Output Data Type (20-port Gb switches)..... 263
Module-defined Input Data Type (20-port switches) 264
Module-defined Output Data Type (20-port switches) 266
Module-defined Input Data Type (24-port switches) 267
Module-defined Output Data Type (24-port switches) 270

Appendix B

Port Assignments for CIP Data 271

Appendix C

Cables and Connectors
10/100 and 10/100/1000 Ports 273
Connect to 10BASE-T- and 100BASE-TX-Compatible Devices 274
Dual-purpose Ports (combo ports)..... 276
Console Ports..... 277
Stratix 5700 Console Ports 277
ArmorStratix 5700 Console Port..... 278
Alarm Ports..... 279
Cable and Adapter Specifications 280
SFP Module Cable Specifications 280
PoE Port Cable Specifications 280
Adapter Pinouts..... 280

Appendix D

History of Changes
1783-UM004D-EN-P, March 2014 283
1783-UM004C-EN-P, December 2013 283
1783-UM004B-EN-P, June 2013..... 285

Index

This publication describes the embedded software features and tools for configuring and managing the Stratix 5700™ Ethernet managed switches. In addition, this publication provides troubleshooting information to help you resolve basic switch and network issues.

Use this manual if you configure and monitor Stratix 5700 Ethernet managed switches. This manual assumes you understand the following:

- Local area network (LAN) switch fundamentals
- Concepts and terminology of the Ethernet protocol and local area networking

Studio 5000 Environment

The Studio 5000 Automation Engineering & Design Environment™ combines engineering and design elements into a common environment. The first element is the Studio 5000 Logix Designer™ application. The Logix Designer application is the rebranding of RSLogix™ 5000 software and will continue to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.

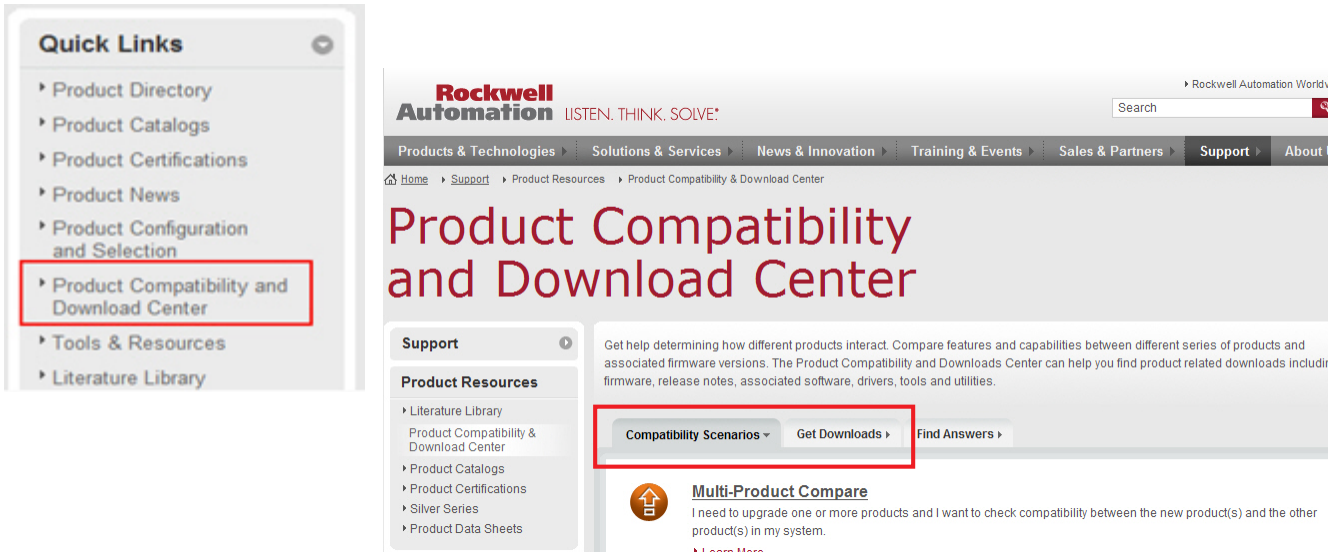
Rockwell Software
Studio 5000
Allen-Bradley • Rockwell Software
Rockwell Automation
Copyright © 2014 Rockwell Automation Technologies, Inc.
All Rights Reserved. This program is protected by U.S. and International copyright laws.

The Studio 5000® environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. The Studio 5000 environment is the one place for design engineers to develop all of the elements of their control system.

Access Product Release Notes

Product release notes are available online within the Product Compatibility and Download Center.

1. From the Quick Links list on http://www.ab.com, choose Product Compatibility and Download Center.


Quick Links
Product Directory
Product Catalogs
Product Certifications
Product News
Product Configuration and Selection
Product Compatibility and Download Center
Tools & Resources
Literature Library
Rockwell Automation LISTEN. THINK. SOLVE.
Search
Products & Technologies
Solutions & Services
News & Innovation
Training & Events
Sales & Partners
Support
Home
Support
Product Resources
Product Compatibility & Download Center
Product Compatibility and Download Center
Support
Product Resources
Literature Library
Product Compatibility & Download Center
Product Catalogs
Product Certifications
Silver Series
Product Data Sheets
Get help determining how different products interact. Compare features and capabilities between different series of products and associated firmware versions. The Product Compatibility and Downloads Center can help you find product related downloads including firmware, release notes, associated software, drivers, tools and utilities.
Compatibility Scenarios
Get Downloads
Find Answers
Multi-Product Compare
I need to upgrade one or more products and I want to check compatibility between the new product(s) and the other product(s) in my system.

2. From the Compatibility Scenarios tab or the Get Downloads tab, search for and choose your product.

3. Click the download icon to access product release notes.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Stratix Ethernet Managed Switches Technical Data, publication 1783-TD001	Provides specification information for the switches.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Provides information about implementing a system based on the EtherNet/IP platform.
Device Manager Web interface online help (provided with the switch)	Provides context-sensitive information on configuring and using the switch, including system messages.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http:/www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

For information on additional software features or further configuration, see these Cisco publications at http://www.Cisco.com:

- Cisco IE-2000 Command Line Reference Manual
- Cisco IE-2000 Software Configuration Guide
- Cisco IE-2000 Switch System Message Guide

Notes:

About the Switches

Topic	Page
Switch Catalog Numbers	16
Switch Software Features	17
Stratix 5700 Switch Dimensions	18
ArmorStratix 5700 Switch Dimensions	21
Switch Front Panel	22
Switch Hardware Features	22
SD Card	23
Switch Memory Allocation	25
Device Manager Web Interface	26
Studio 5000 Environment	27
Cisco Network Assistant	27
Command Line Interface	28

Stratix 5700 Ethernet managed switches provide a secure switching infrastructure for harsh environments. You can connect these switches to network devices such as servers, routers, and other switches. In industrial environments, you can connect Ethernet-enabled industrial communication devices, including programmable logic controllers (PLCs), human-machine interfaces (HMIs), drives, sensors, and I/O.

Switch Catalog Numbers

These switches are available with either lite or full firmware.

Catalog Number	Description
Stratix 5700 Switches	
1783-BMS4S2SGL	6 SFP-port (4 Ethernet ports; 2 Gigabit ports) managed switch; lite firmware
1783-BMS4S2SGA	6 SFP-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware
1783-BMS06SL	6-port (4 Ethernet ports; 2 SFP slots) managed switch; lite firmware
1783-BMS06SA	6-port (4 Ethernet ports; 2 SFP slots) managed switch; full firmware
1783-BMS06TL	6-port (6 Ethernet ports) managed switch; lite firmware
1783-BMS06TA	6-port (6 Ethernet ports) managed switch; full firmware
1783-BMS06SGL	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; lite firmware
1783-BMS06SGA	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; full firmware
1783-BMS06TGL	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware
1783-BMS06TGA	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware
1783-BMS10CL	10-port (8 Ethernet ports; 2 combo ports) managed switch; lite firmware
1783-BMS10CA	10-port (8 Ethernet ports; 2 combo ports) managed switch; full firmware
1783-BMS10CGL	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; lite firmware
1783-BMS10CGA	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware
1783-BMS10CGN	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; network address translation (NAT)
1783-BMS10CGP	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; PTP
1783-BMS12T4E2CGNK	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware; NAT; conformal coating
1783-BMS12T4E2CGP	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware, PTP
1783-BMS12T4E2CGL	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; lite firmware
1783-BMS20CL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; lite firmware
1783-BMS20CA	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; full firmware
1783-BMS20CGL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; lite firmware
1783-BMS20CGN	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; NAT
1783-BMS20CGP	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP
1783-BMS20CGPK	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP; conformal coating
ArmorStratix™ 5700 Switches	
1783-ZMS8TA	8-port (8 Ethernet ports) managed switch; full firmware
1783-ZMS16TA	16-port (16 Ethernet ports) managed switch; full firmware
1783-ZMS24TA	24-port (24 Ethernet ports) managed switch; full firmware
1783-ZMS4T4E2TGP	10-port (4 Ethernet ports; 4 PoE/PoE+ ports; 2 Gigabit ports) managed switch; full firmware; Precision Time Protocol (PTP)
1783-ZMS8T8E2TGP	18-port (8 Ethernet ports; 8 PoE/PoE+ ports; 2 Gigabit ports) managed switch; full firmware; PTP
SFP Modules	
1783-SFP100FX	100BASE-FX multi-mode fiber transceiver
1783-SFP1GSX	1000BASE-SX multi-mode fiber transceiver
1783-SFP100LX	100BASE-LX single-mode fiber transceiver
1783-SFP1GLX	1000BASE-LX single-mode fiber transceiver

Catalog Number	Description
Power Supply	
1606-XL series (recommended) 1606-XLP series (recommended) or equivalent	Class 2, 24V DC output power supplies
SD Card	
1784-SD1	1 GB Industrial SD card

Switch Software Features

These software features are available with the Stratix 5700 switches.

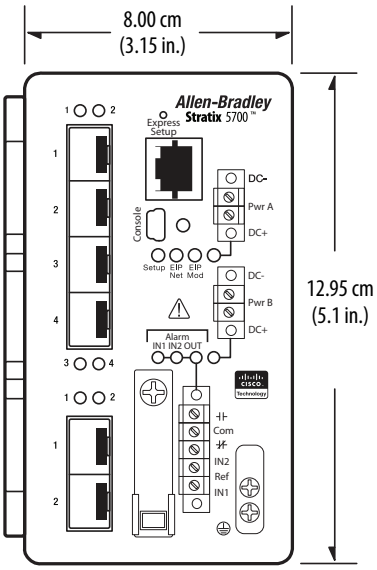
Feature	Lite Firmware	Full Firmware
CIP Sync (IEEE 1588)		Separate option
Resilient Ethernet Protocol (REP)	•	•
FlexLinks		•
Quality of Service (QoS)		•
STP, RSTP, MST (instances)	64	128
IGMP Snooping with querier	•	•
VLANs with trunking	64	255
EtherChannel (link aggregation)		•
Port Threshold (Storm Control and Traffic Shaping)		•
IPv6 support		•
Access Control Lists (ACL)		•
Static and interVLAN routing		•
CIP port control and fault detection	•	•
MAC ID Port security		•
IEEE 802.1x security		•
TACACS+, RADIUS authentication	•	•
Encryption (SSH, SNMPv3, HTTPS)		Separate IOS firmware available as a separate catalog item
Port mirroring	•	•
Syslog	•	•
Broken wire detection	•	•
Duplicate IP address detection		•
SNMP	•	•
Smartports	•	•
DHCP per port	•	•
Command line interface (CLI)	•	•

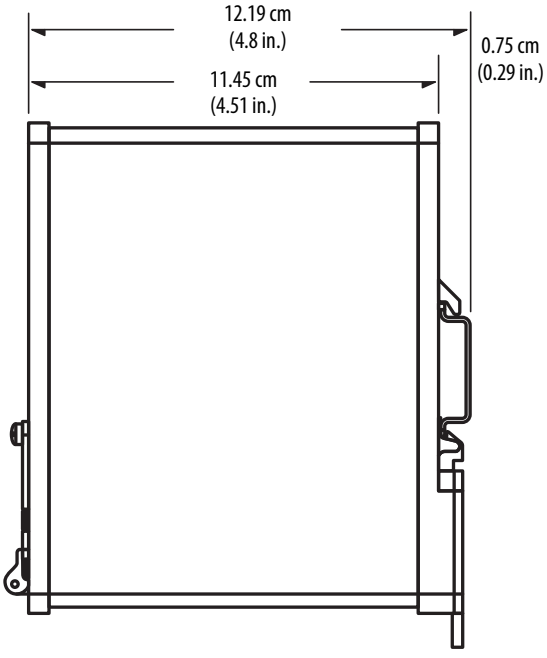
Feature	Lite Firmware	Full Firmware
Compatible with Cisco tools: Cisco Network Assistant (CNA); CiscoWorks	•	•
EtherNet/IP (CIP) interface	•	•
Network address translation (NAT)		Separate option

Stratix 5700 Switch Dimensions

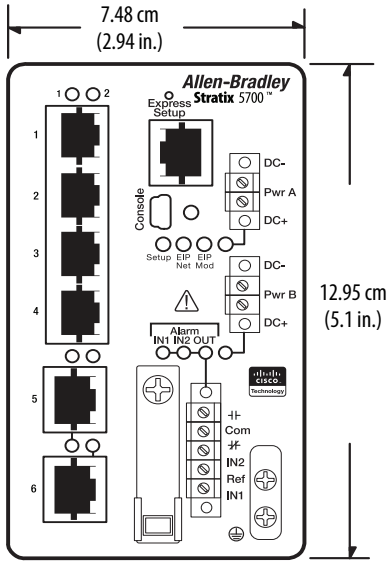
These diagrams are representative of the switches. Actual faceplates vary depending on the catalog number.

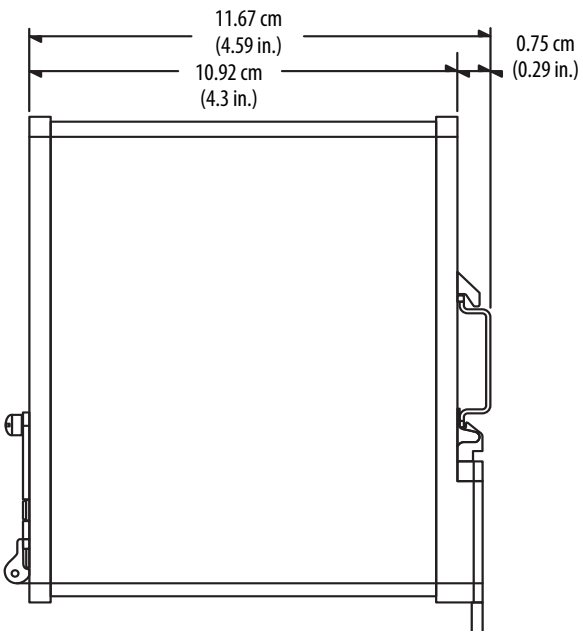
6 SFP-port Switches
1783-BMS4S2SGL, 1783-BMS4S2SGA



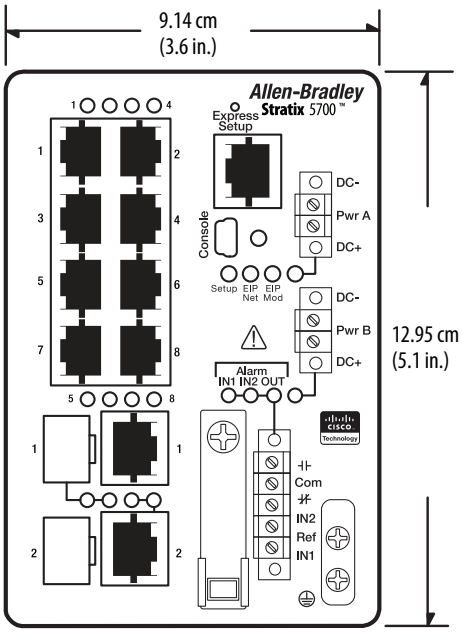


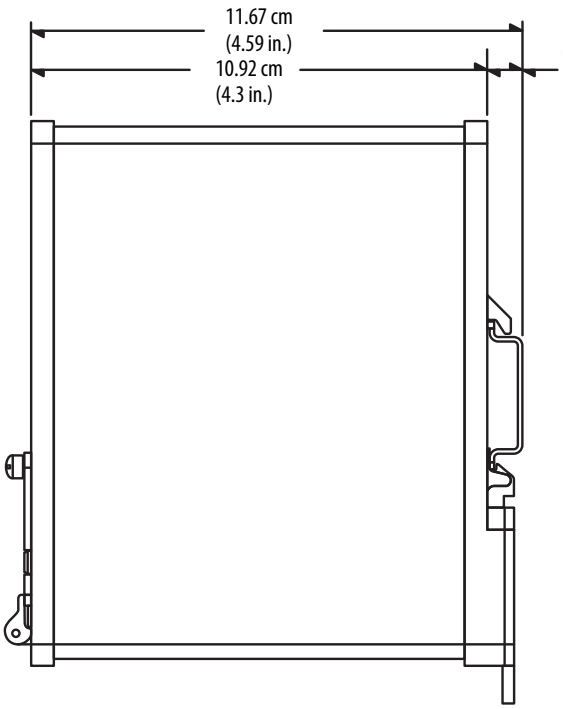
6-port Switches
1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA, 1783-BMS06SGL, 1783-BMS06SGA, 1783-BMS06TGL, 1783-BMS06TGA



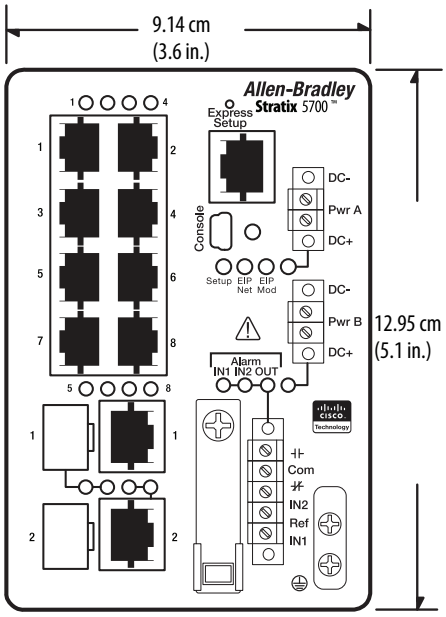


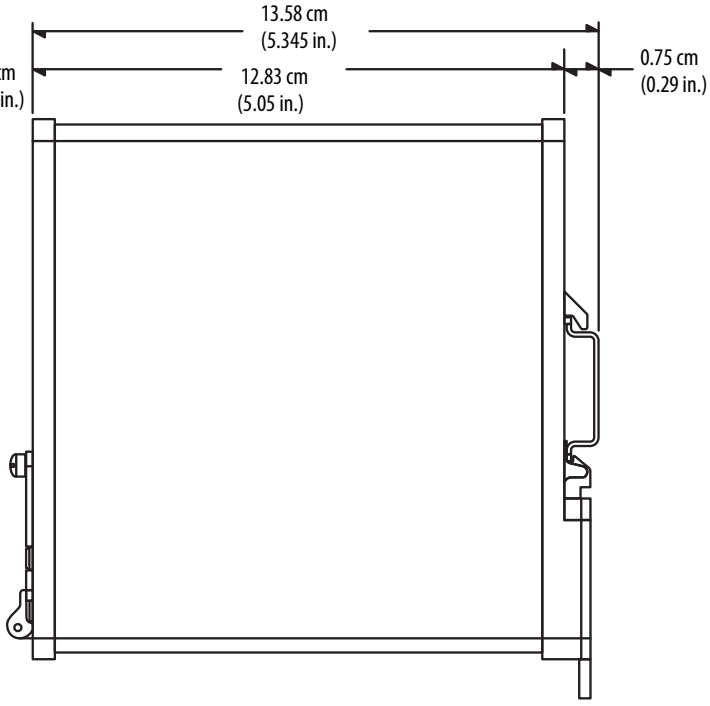
10-port Switches
1783-BMS10CL, 1783-BMS10CA,
1783-BMS10CGL, 1783-BMS10CGA





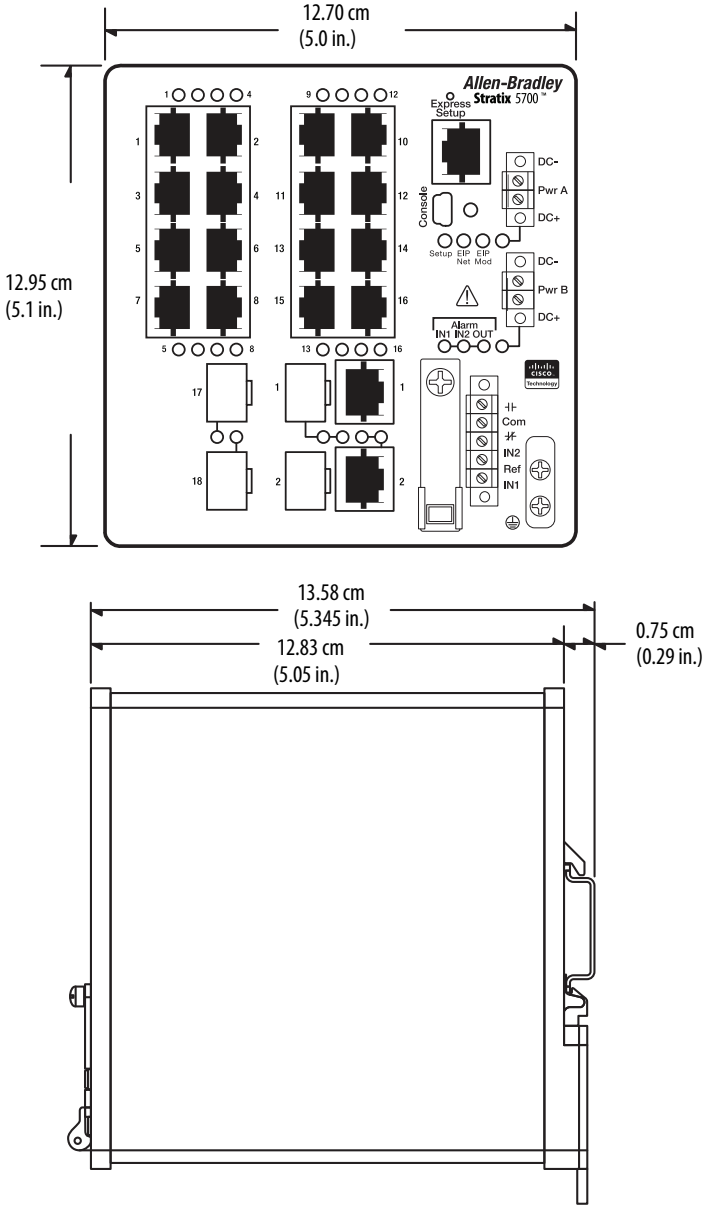
10-port Switch
1783-BMS10CGP, 1783-BMS10CGN





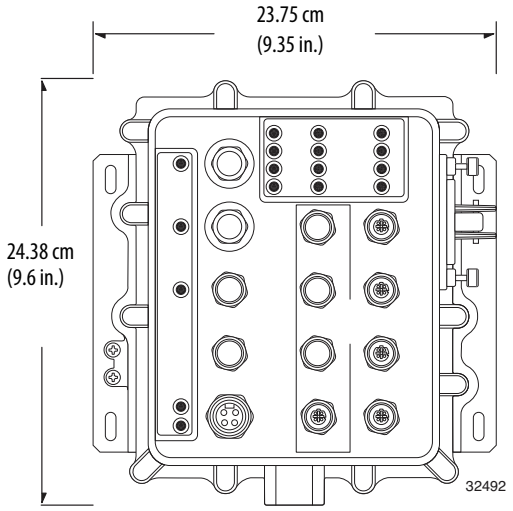
18- and 20-port Switches

1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGL, 1783-BMS20CL, 1783-BMS20CA, 1783-BMS20CGL, 1783-BMS20CGP, 1783-BMS20CGN, 1783-BMS20CGPK

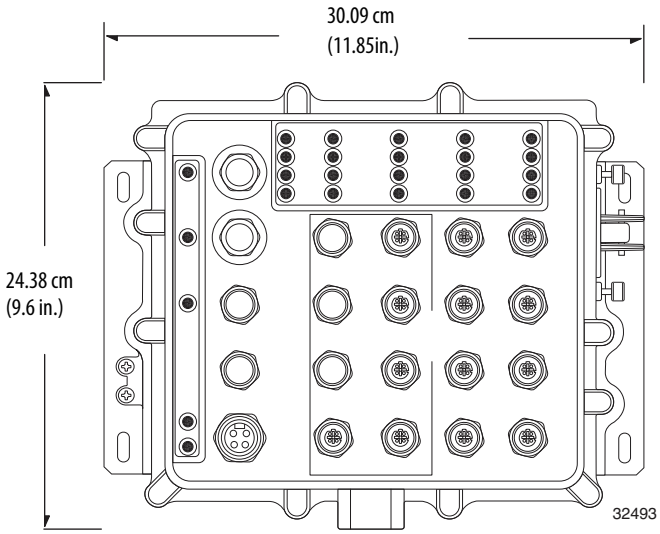


ArmorStratix 5700 Switch Dimensions

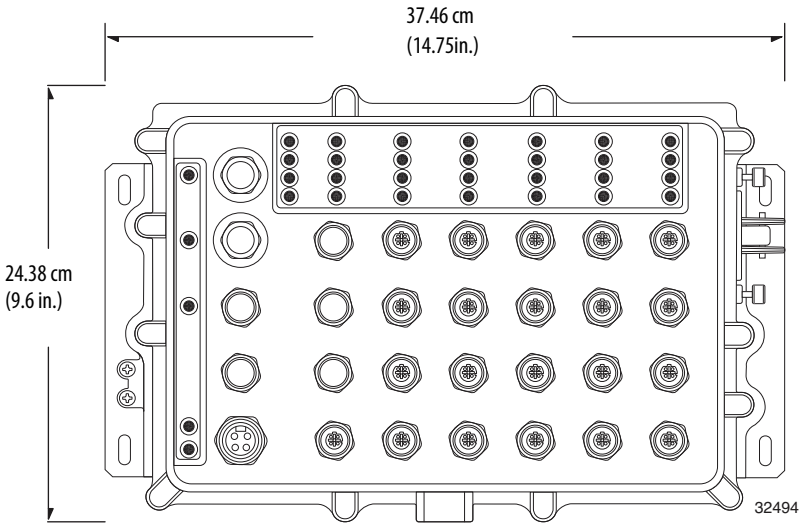
8-port Switches
1783-ZMS8TA, 1783-ZMS4T4E2TGP



16-port Switches
1783-ZMS16TA, 1783-ZMS8T8E2TGP



24-port Switch
1783-ZMS24TA

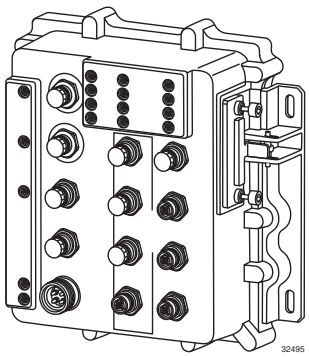


Switch Front Panel

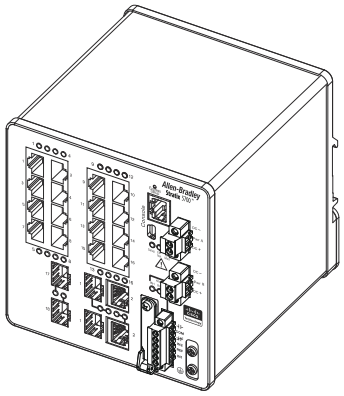
The switch front panel contains the ports, status indicators, and power and relay connectors.

These diagrams are representative of the switch front panels. Actual front panels vary depending on the catalog number.

ArmorStratix 5700 Switch



Stratix 5700 Switch



32276-M

Switch Hardware Features

These hardware features are available with the switches.

Feature	Description
Power and relay connectors	You connect the DC power and alarm signals to the switch through two front panel connectors. One connector provides primary DC power (Pwr A) and a second connector (Pwr B) provides secondary power. The two connectors are physically identical and are on the right side of the front panel. The 6-pin alarm connector provides an interface for an output alarm relay and two input alarms. The output alarm can be activated for environmental, power supply, and port status alarm conditions and can be configured to indicate an alarm with one normally open and one normally closed (form C) contact. From the CLI, you can configure the output alarm to be normally energized or normally de-energized. The input alarm terminals can be used to activate alarms for any conditions external to the switch. The switch can operate with a single power source or with dual power sources. When both power sources are operational, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch.
Console port	For configuring, monitoring, and managing the switch, you can connect a switch to a computer through the console port and a RJ45-to-DB-9 adapter cable or a mini USB cable (neither cables are supplied with the switch). The mini USB driver is available in the firmware download section at http://www.rockwellautomation.com.
Dual-purpose uplink ports	The two dual-purpose uplink ports available on some models can each be configured for RJ45 (copper) or SFP (fiber) media types. Only one of these connections in each of the dual-purpose ports can be active at a time. If both ports are connected, the SFP module port has priority. You can set the copper RJ45 ports to operate at 10, 100, or 1000 Mbps (1000Mbps is not supported on all modules with combo ports), full-duplex or half-duplex. You can configure them as fixed 10, 100, or 1000 Mbps (Gigabit) Ethernet ports and can configure the duplex setting. You can use approved Gigabit (or 100 Mbps) Ethernet SFP modules to establish fiber-optic connections to other switches. These transceiver modules are field-replaceable, providing the uplink interfaces when inserted in an SFP module slot. You use fiber-optic cables with LC connectors to connect to a fiber-optic SFP module. These ports operate only in full-duplex.
10/100 ports	You can set the 10/100 ports to operate at 10 or 100 Mbps, full-duplex or half-duplex. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3-2002. (The default setting is autonegotiate.) When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch.

Feature	Description
100BASE-FX/SX ports	The IEEE 802.3-2002 100BASE-FX ports provide full-duplex, 100 Mbps connectivity over multi-mode fiber (MMF) cables. These ports use a built-in, small-form-factor fixed (SFF) fiber-optic transceiver module that accepts a dual LC connector.
1000BASE-FX/SX ports	The IEEE 802.3-2002 1000BASE-FX ports on some models provide full-duplex, 1 Gbps connectivity over multi-mode fiber (MMF) cables. These ports use a built-in, small-form-factor fixed (SFF) fiber-optic transceiver module that accepts a dual LC connector.
PoE ports	The PoE ports available on some models can be configured for PoE (IEEE 802.3af) or PoE+ (IEEE 802.3at Type 2): • For PoE configuration, the PoE ports require an external, 2-wire 48V DC input power source. • For PoE+ configuration, the PoE ports require an external, 2-wire 54V DC input power source.
Auto-MDIX	When connecting the switch to workstations, servers, and routers, straight-through cables are normally used. However, the automatic medium-dependent interface crossover (auto-MDIX) feature of the switch is enabled by default and automatically reconfigures the ports to use either a straight-through or crossover cable type. The Auto-MDIX feature is enabled by default. When the auto-MDIX feature is enabled, the switch detects the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly. You can use the command-line interface (CLI) to disable the auto-MDIX feature. See the online help for more information.

Configuration Files

The switch configuration file (config.txt) is in ASCII human-readable format. This configuration file is stored in nonvolatile memory and is read into the switches' Random Access Memory (RAM) as the running configuration when the switch is powered up. When any changes are made to the configuration, the changes immediately take effect in the running configuration. The Device Manager Web interface and the Add-on Profile (AOP) for the Logix Designer application automatically write changes to flash memory to be retained for the next power-up cycle. Any changes made via the CLI must be manually written to flash memory to be retained for the next power-up cycle.

SD Card

The switch is equipped with a slot for an optional Secure Digital (SD) card, in addition to the onboard flash memory. The SD card can be used instead of onboard flash memory to easily restore a switch configuration in case of failure or to easily duplicate configurations when you are deploying a new network.

If the SD card is installed on the switch, the switch starts the IOS and configuration present on the SD card. If the SD card is not installed, or files are not present, the switch reads the on-board boot parameters and restarts from the specified IOS image on the onboard flash memory.

You must use the SD card available from Rockwell Automation (catalog number 1784-SD1) with the switch.

ATTENTION: Rockwell Automation reserves the right to withhold support if a non-Rockwell SD card is used in this product.

If you start from the SD card and then remove it while the switch is running, the following conditions apply:

- The Device Manager Web interface is no longer be accessible.
- Changes made by using the CLI or the AOP take effect, but are not saved when the switch is restarted.
- If the SD card is reinserted into the slot, changes are not saved to the card unless new changes are made. Then the entire configuration is saved to the card.

ATTENTION: SD cards commonly have a physical read-only lock switch. If this switch is engaged, the switch starts from the SD card successfully. Changes made by using the CLI, AOP, or Device Manager Web interface take effect, but are not saved when the switch is restarted.

SD Card Sync

You can use the Device Manager Web interface or the AOP for the Logix Designer application to synchronize the SD card for configuration and IOS updates. The configuration synchronization process synchronizes config.text and vlan.dat from the chosen source to the chosen destination.

The IOS image synchronization process synchronizes the existing bootable IOS image from the chosen source to the chosen destination. This process takes approximately five minutes to complete.

If other files, such as backup configurations, are present on the SD card, they are not synchronized.

ATTENTION: When synchronizing, be aware of your start-up source, so that you know which way to synchronize. Device Manager provides this information on the SD Card Sync tab. You can overwrite your desired configuration if you synchronize in the wrong direction.

Switch Memory Allocation

The following table provides details on default memory allocation for the switches.

You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions; for example, use the default template to balance resources, and use access template to obtain maximum ACL usage. To allocate hardware resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features.

The following SDM Templates are available:

- Default
- Routing
- Dual IPv4 and IPv6

Consider using the routing template if you enable static routing, or if you have more than 180 IGMP groups or multicast routes. Consider using the Dual IPv4 and IPv6 template if you are using IPv6.

You can select SDM templates for IP version 4 (IPv4) to optimize these features.

Feature	Memory Allocation		
	Default	Routing	Dual IPv4 and IPv6
Unicast MAC addresses	8 K	4 K	7.5 K
IPv4 IGMP groups + multicast routes	0.25 K	0.25 K	0.25 K
IPv4 unicast routes	0	4.25 K	0
IPv6 multicast groups	0	0	0.375 K
Directly connected IPv4 hosts	0	4 K	
Directly connected IPv6 addresses	0	0	o
Indirect IPv4 routes	0	0.25 K	
Indirect IPv6 routes	0	0	0
IPv4 policy based routing aces	0	0	
IPv4/MAC QoS aces	0.375 K	0.375 K	0.375 K
IPv4/MAC security aces	0.375 K	0.375 K	0.375 K
IPv6 policy based routing aces	0	0	0
IPv6 QOS aces	0	0	0
IPv6 security aces	0	0	0.125 K

Device Manager Web Interface

You can manage the switch by using the Device Manager Web interface to configure and monitor the switch. The Device Manager Web interface is a graphical device management tool for configuring, monitoring, and troubleshooting individual switches.

The Device Manager Web interface displays real-time views of switch configuration and performance. It simplifies configuration tasks with features such as Smartports to quickly set up the switch and its ports. It uses graphical, color-coded displays, such as the Front Panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert tools to help you to identify and to solve networking problems.

You can display the Device Manager Web interface from anywhere in your network through a Web browser such as Microsoft Internet Explorer.

Hardware Requirements

Attribute	Requirement
Processor speed	1 GHz or faster (32-bit or 64-bit)
RAM	1 GB (32-bit) or 2 GB (64-bit)
Available hard drive space	16 GB (32-bit) or 20 GB (64-bit)
Number of colors	256
Resolution	1024 x 768
Font size	Small

Software Requirements

Web Browser	Version
Microsoft Internet Explorer	9.0, 10.0, or 11.0 with JavaScript enabled
Mozilla Firefox	25 or 26 with JavaScript enabled

The Device Manager Web interface verifies the browser version when starting a session to be sure that the browser is supported.

TIP So that the Device Manager Web interface runs properly, disable any pop-up blockers or proxy settings in your browser software and any wireless clients running on your computer or laptop.

Studio 5000 Environment

You can manage the switch by using the Logix Designer application in the Studio 5000 environment. The Logix Designer application is IEC 61131-3 compliant and offers relay ladder, structured text, function block diagram, and sequential function chart editors for you to develop application programs.

Hardware Requirements

Attribute	Requirement
Processor speed	Pentium II 450 MHz min Pentium III 733 MHz (or better) recommended
RAM	128 MB min 256 MB recommended
Free hard drive space	3 GB
Optical drives	DVD
Video requirements	256-color VGA graphics adapter 800 x 600 min resolution (True Color 1024 x 768 recommended)
Resolution	800 x 600 min resolution (True Color 1024 x 768 recommended)

Cisco Network Assistant

Cisco Network Assistant is a Web interface that you download from Cisco's website and run on your computer. It offers advanced options for configuring and monitoring multiple devices, including switches, switch clusters, switch stacks, routers, and access points.

To use the software, follow these steps.

1. Go to http://www.cisco.com/go/NetworkAssistant.

   You must be a registered user, but you need no other access privileges.
2. Find the Network Assistant installer.
3. Download the Network Assistant installer, and run it.

   You can run it directly from the Web if your browser offers this choice.
4. When you run the installer, follow the displayed instructions.
5. In the final panel, click Finish to complete the Network Assistant installation.
6. See the Network Assistant online help for more information.

Command Line Interface

You can manage the switch from the command line interface (CLI) by connecting your personal computer directly to the switch console port or through the network by using Telnet.

To access the CLI through the console port, follow these steps.

1. Connect to the console port in one of these ways:
   - Use a RJ45-to-DB-9 adapter cable (not supplied with the switch) to connect to the standard 9-pin serial port on a personal computer.
   - Use a standard mini-USB cable (not supplied with the switch) to connect to the mini-USB port on a personal computer.
   - If you are using the USB cable, download the drivers for your Microsoft Windows computer from http://www.rockwellautomation.com.
2. Connect the other end of the cable to the console port on the switch.

WARNING: The console port is intended only for temporary local programming purposes and not intended for permanent connection. If you connect or disconnect the console cable with power applied to this module or the programming device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

3. Start a terminal-emulation program on the personal computer.
4. Configure the personal computer terminal emulation software for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Switch Installation

Topic	Page
Stratix 5700 Switch Installation	**30**
Installation Guidelines	31
Install or Remove the SD Card (optional)	33
Verify Switch Operation	34
Mount the Switch on a DIN Rail	36
Remove the Switch from the DIN Rail	38
Ground the Switch	38
Wire the Switch DC Power Source	40
Attach the Switch Power Connectors	43
Wire the Power over Ethernet DC Power Source	44
Attach the PoE Power Connector	46
Install an SFP Module (optional)	46
Remove SFP Modules from SFP Module Slots	48
Wire the External Alarms	49
Attach the Alarm Relay Connector to the Switch	52
Connect to 10/100 and 10/100/1000 Ports	52
Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports	53
Connect to PoE Ports	54
Connect to SFP Modules	55
Connect to a Dual-purpose Port	56
ArmorStratix 5700 Switch Installation	**57**
Installation Guidelines	57
Install or Remove the SD Card (optional)	59
Verify Switch Operation	60
Mount the Switch	61
Ground the Switch	62
Connect the Switch to a DC Power Source	64
Wire External Alarms	65
Connect to 10/100 and 10/100/1000 Ports	66
Connect to PoE Ports	66
Set Up the Switch Initially with Express Setup	**67**

Stratix 5700 Switch Installation

ATTENTION: Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame spread rating of 5VA or be approved for the application if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations.	**Informations sur l'utilisation de cet équipement en environnements dangereux.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués "CL I, DIV 2, GP A, B, C, D" ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNING: RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

European Hazardous Location Approval

The following applies when the product bears the Ex Marking.

This equipment is intended for use in potentially explosive atmospheres as defined by European Union Directive 94/9/EC and has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of Category 3 equipment intended for use in Zone 2 potentially explosive atmospheres, given in Annex II to this Directive. Compliance with the Essential Health and Safety Requirements has been assured by compliance with EN 60079-15 and EN 60079-0.

ATTENTION: This equipment is not resistant to sunlight or other sources of UV radiation.

WARNING:

- This equipment shall be mounted in an ATEX-certified enclosure with a minimum ingress protection rating of at least IP54 (as defined in IEC60529) and used in an environment of not more than Pollution Degree 2 (as defined in IEC 60664-1) when applied in Zone 2 environments. The enclosure must have a tool-removable cover or door.
- This equipment shall be used within its specified ratings defined by Rockwell Automation.
- Provision shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140% of the rated voltage when applied in Zone 2 environments.
- Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.
- Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.

Installation Guidelines

WARNING: If you connect or disconnect Ethernet cables with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: The alarm port cables are not to exceed 10.0 m (32.81 ft).

At the end of its life, this equipment should be collected separately from any unsorted municipal waste.

When determining where to place the switch, observe these guidelines:

- Airflow around the switch is unrestricted. To prevent the switch from overheating, observe the following minimum clearances:
  - Top and bottom: 50.8 mm (2.0 in.)
  - Sides: 50.8 mm (2.0 in.)
  - Front: 50.8 mm (2.0 in.)

- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 100 m (328 ft).
- The fiber-optic cable length from a switch to an attached device cannot exceed the distance specified in Appendix C.
- For maximum noise immunity, shielded cables must be used on the RJ45 uplink ports (Gi1/1 and Gi1/2) on these switches:
  - 1783-BMS06TGL
  - 1783-BMS06TGA
  - 1783-BMS10CGL
  - 1783-BMS10CGA
  - 1783-BMS10CGN
  - 1783-BMS10CGP
  - 1783-BMS12T4E2CGNK
  - 1783-BMS12T4E2CGP
  - 1783-BMS12T4E2CGL
  - 1783-BMS20CGL
  - 1783-BMS20CGN
  - 1783-BMS20CGP
  - 1783-BMS20CGPK
- Temperature surrounding the unit does not exceed 60 °C (140 °F).

IMPORTANT	When the switch is installed in an industrial enclosure, the temperature within the enclosure is greater than normal room temperature outside the enclosure. The temperature inside the enclosure cannot exceed 140 °F (60 °C), the maximum ambient enclosure temperature of the switch.

- Clearance to front and rear panels meets these conditions:
  - Front-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm relay connector are within reach of the connection to the DC power source.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Connect the unit to only a Class 2 DC power source.

ATTENTION: Do not wire more than 1 conductor on any single terminal.

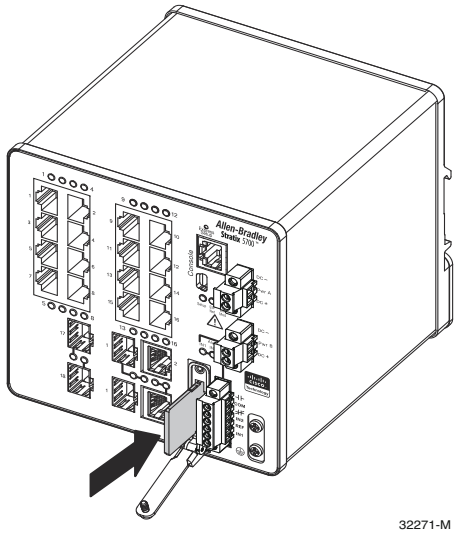
Install or Remove the SD Card (optional)

WARNING: When you insert or remove the CompactFlash/SD memory card while power is on, an electrical arc can occur. This can cause an explosion in hazardous location installations.

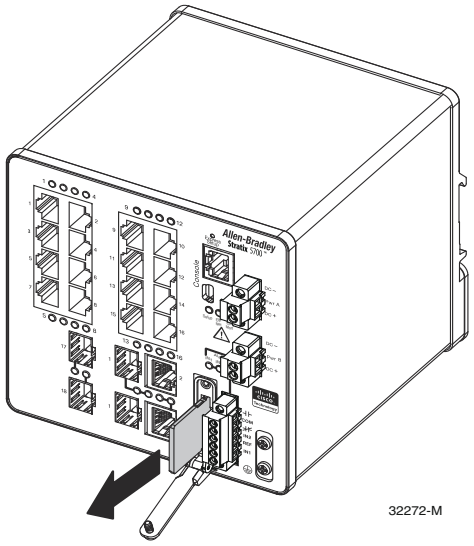
Be sure that power is removed or the area is nonhazardous before proceeding.

To install or replace the SD card, follow these steps.

1. On the front of the switch, locate the door that protects the SD card slot.
2. Loosen the captive thumb screw at the top of the door by using a screwdriver to open the door.
3. Install or remove the card:
   - To install the card, slide it into the slot, and press it firmly in place until it latches in the spring loaded mechanism. The card is keyed so that you cannot fully insert it the wrong way.



- To remove the card, push it in and let it pop out via the spring-loaded mechanism. Grasp the card top and pull it out. Place it in an antistatic bag to protect it from static discharge.



4. Close the guard door and fasten the captive screw by using a screwdriver to keep the door in place.

Verify Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up.

The time required for the switch to start up is directly related to your switch configuration. Start time is negatively affected by such things as the following:

- Spanning Tree Learning mode
- Number of files or images in onboard flash memory

To test the switch, follow these steps.

1. Apply power to the switch.

   To apply power to a switch that is directly connected to a DC power source, locate the circuit breaker on the panel board that services the DC circuit, and switch the circuit breaker to the ON position.

2. Verify the start-up sequence.

   When you power on the switch, it automatically begins a start-up routine. The System status indicator blinks green as the IOS software image loads. If the routine fails, the System status indicator turns red.

   IMPORTANT Start-up failures are usually fatal to the switch. Contact your Rockwell Automation representative immediately if your switch does not complete the start sequence successfully.

   IMPORTANT You can disable boot fast and run the Power-on Self Test (POST) by using the IOS CLI. See the appropriate documentation at http://www.Cisco.com for more information.

3. After successfully running this test, do the following:
   a. Turn off power to the switch.
   b. Disconnect the cables.
   c. Decide where you want to install the switch

Mount the Switch on a DIN Rail

The switch ships with a spring-loaded latch on the rear panel for mounting on a DIN rail.

WARNING: If you connect or disconnect console port cables with power applied to this module or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

WARNING: Do not use the USB-mini console port in hazardous locations.

ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wriststrap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.

ATTENTION: This equipment is supplied as open type equipment. It must be mounted within an enclosure suitably designed for those specific environmental conditions and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by using a tool.

The enclosure must meet IP 54 or NEMA type 4 minimum enclosure rating standards.

ATTENTION: To prevent the switch from overheating, make sure these minimum clearances:

- Top and bottom: 50.8 mm (2.0 in.)
- Exposed side (not connected to the module): 50.8 mm (2.0 in.)
- Front: 50.8 mm (2.0 in.)

ATTENTION: The console ports are intended for temporary local programming purposes only and not intended for permanent connection.

The console port cables are not to exceed 3.0 m (9.84 ft) and must not contain hubs.

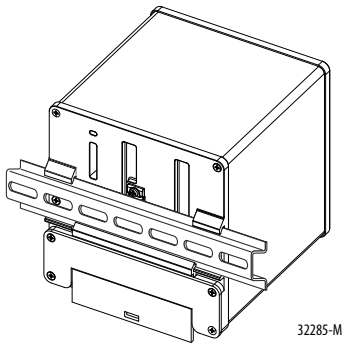
ATTENTION: Under certain conditions, viewing the optical port may expose the eye to hazard. When viewed under some conditions, the optical port may expose the eye beyond the maximum permissible exposure recommendations.

ATTENTION: Class 1 laser product. Laser radiation is present when the system is open and interlocks bypassed. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

ATTENTION: This product is grounded through the DIN rail to chassis ground. Use zinc plated yellow-chromate steel DIN rail to assure proper grounding. The use of other DIN rail materials (for example, aluminum or plastic) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) and use end-anchors appropriately.

To attach the switch to a DIN rail, follow these steps.

1. Position the rear panel of the switch directly in front of the DIN rail, making sure that the DIN rail fits in the space between the two hooks near the top of the switch and the spring-loaded latch near the bottom.
2. Holding the bottom of the switch away from the DIN rail, place the two hooks on the back of the switch over the top of the DIN rail.

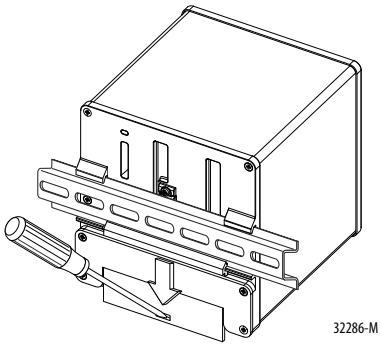


3. Push the switch toward the DIN rail to cause the spring loaded latch at the bottom rear of the switch to move down and snap into place.

Remove the Switch from the DIN Rail

To remove the switch from a DIN rail or a rack, follow these steps.

1. Remove power from the switch, and disconnect all cables and connectors from the front panel of the switch.
2. Insert a tool, such as a flat-head screwdriver, in the slot at the bottom of the spring-loaded latch and use it to release the latch from the DIN rail.



Ground the Switch

For DC power connections, use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

WARNING: If you connect or disconnect power or alarm wiring while the field-side power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

This equipment is intended to be grounded to comply with emission and immunity requirements. Make sure that the switch functional ground lug is connected to earth ground during normal use.

ATTENTION: To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions and use a suitable ring terminal lug, such as Thomas & Betts part number 10RCR or equivalent.

ATTENTION: For proper grounding, you must always connect the power supply functional-ground screw when connecting the power supply. You must provide an acceptable grounding path for each device in your application. For more information on proper grounding guidelines, refer to publication 1770-4.1, Industrial Automation Wiring and Grounding Guidelines.

Use at least 4 mm^2 (12 AWG) wire to connect to the external grounding screw.

The ground lug is not supplied with the switch. You can use one of the these options:

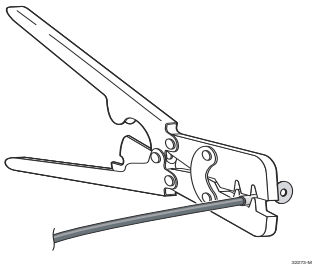
- Single ring terminal
- Two single ring terminals

To ground the switch to earth ground, follow these steps. Be sure to follow any grounding requirements at your site.

1. Use a Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the front panel of the switch.

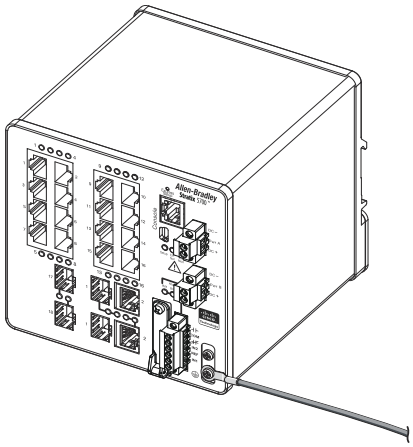
   Store the ground screw for later use.
2. Use the manufacturer's guidelines to determine the wire length to be stripped.
3. Insert the ground wire into the ring terminal lug and use a crimping tool to crimp the terminal to the wire.

   If you are using two ring terminals, repeat this action for the second ring terminal.



4. Slide the ground screw through the terminal.

5. Insert the ground screw into the functional ground screw opening on the front panel.



6. Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal lugs to the switch front panel to 0.4 N•m (3.5 lb•in).

   Do not exceed the recommended torque.

7. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

Wire the Switch DC Power Source

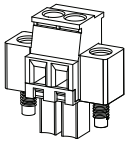
To wire the DC power source for the switch, follow these steps.

ATTENTION: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding:

- This product is intended to be supplied by a Class 2 power source marked with 'Class 2' and rated from 12, 24, or 48V DC, 2.5 A.
- To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).
- A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.
- This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that the protective device is rated not greater than 3 A.
- Installation of the equipment must comply with local and national electrical codes.
- Allow only trained and qualified personnel to install, replace, or service this equipment.

ATTENTION: For wire connections to the power and relay connector, you must use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

1. Locate the power connector.



32280-M

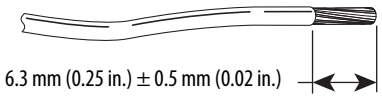
2. Identify the positive and return DC power connections.

   The positive DC power connection is labeled DC+, and the negative DC power connection is the adjacent connection labeled DC-.

3. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.

4. Use an 18-gauge wire-stripping tool to strip each of the two wires to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

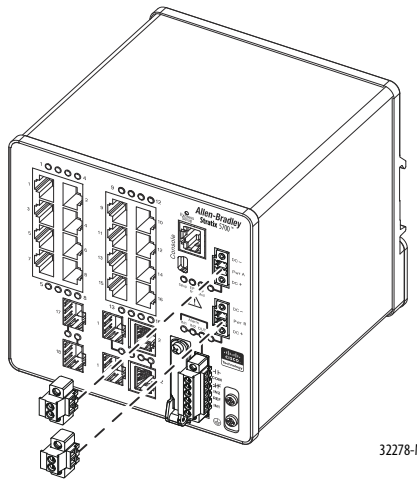
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave wire exposed after installation.



31789-M

5. Loosen the two captive screws that attach the power connector to the switch, and remove the power connector.

   Remove both connectors if you are connecting to two power sources.

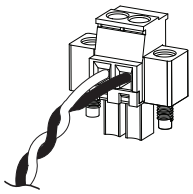


32278-M

6. Insert the exposed part of the positive wire into the connection labeled DC+ and the exposed part of the return wire into the connection labeled DC-.

   Be sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.

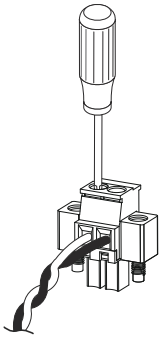
> **ATTENTION:** An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the connector(s) or terminal blocks.



32279-M

7. Use a ratcheting-torque screwdriver to torque the power connector captive screws (above the installed wire leads) to 0.23 N•m (2.0 lb•in).

   Do not exceed the recommended torque.

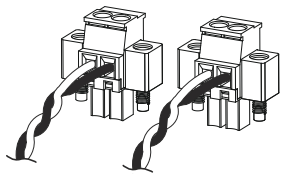


32281-M

8. Connect the other end of the positive wire to the positive terminal on the DC power source, and connect the other end of the return wire to the return terminal on the DC power source.

   When you are testing the switch, one power connection is sufficient. If you are installing the switch and are using a second power source, repeat this procedure with the second power connector.

   The following figure shows the completed DC input wiring on a power connector for a primary power source and an optional secondary power source.

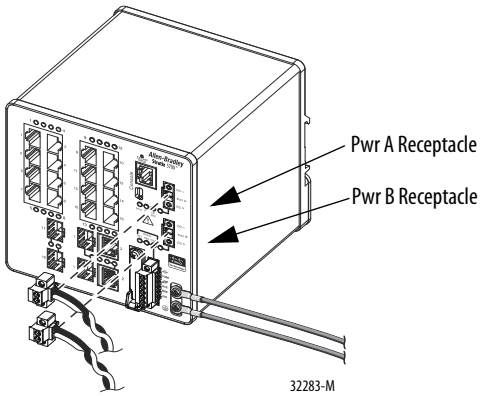


32282-M

Attach the Switch Power Connectors

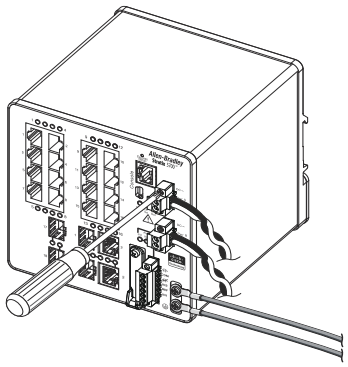
To attach the switch power connectors to the front panel of the switch, follow these steps.

1. Insert one power connector into the Pwr A receptacle on the switch front panel, and the other into the Pwr B receptacle.



32283-M

2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the power connectors.



32284-M

When you are testing the switch, one power source is sufficient. If you are installing the switch and are using a second power source, repeat this procedure for the second power connector (Pwr B), which installs just below the primary power connector (Pwr A).

3. When you are installing the switch, secure the wires coming from the power connectors to the rack by using tie wraps.

Wire the Power over Ethernet DC Power Source

This procedure applies only to switches with PoE ports.

WARNING: The console port is intended only for temporary local programming purposes and not intended for permanent connection. If you connect or disconnect the console cable with power applied to this module or the programming device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: To comply with the CE Low Voltage Directive (LVD), this equipment must be powered from a source compliant with the safety extra low voltage (SELV) or protected extra low voltage (PELV).

To comply with UL restrictions, this equipment must be powered from a source compliant with Class 2 or Limited Voltage/Current.

The switch must be wired and grounded.

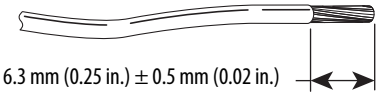
Power supply requirements depend on your application.

Application	Power Supply per Port	Power Consumption	Allen-Bradley Products
PoE only IEEE 802.3af	44…57V DC (48V DC nom)	15.4 W, max	Switched mode power supplies: • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE and PoE + IEEE 802.3at Type 2	50…57V DC (54V DC nom)	15.4 W, max for PoE 30 W, max for PoE+	

WARNING: Before performing any of the following procedures, make sure that power is removed from the DC circuit or the area is nonhazardous before proceeding.

1. Measure a length of 0.82...0.52 mm^2 (18...20 AWG) copper wire long enough to connect to the DC power source.
2. Using an 18-gauge wire-stripping tool, strip each of the two wires to 6.3mm (0.25 in.) ± 0.5 mm (0.02 in.).

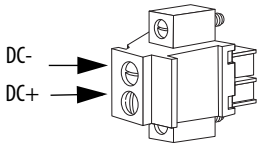
   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wire. Stripping more than the recommended amount of wire can leave wire exposed after installation.



31789-M

3. Locate the power connector.
4. Insert the exposed part of the positive wire into the DC+ connection and the exposed part of the return wire into the DC- connection.

   Make sure that you cannot see any wire lead. Only wire with insulation can extend from the connector.



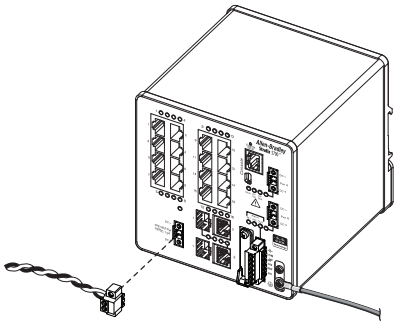
5. Use a ratcheting-torque screwdriver to torque the power connector captive screws (above the installed wire leads) to 0.23 N•m (2.0 lb•in).
6. Connect the other end of the positive wire (the one connected to DC+) to the positive terminal on the DC power source, and connect the other end of the return wire (the one connected to DC-) to the return terminal on the DC power source.

ATTENTION: If multiple power sources are used, do not exceed the specified isolation voltage.

Attach the PoE Power Connector

This procedure applies only to switches with PoE ports.

1. Insert the power connector into the DC input terminal block on the switch front panel.
2. Use a screwdriver to tighten the captive screws on the sides of the power connector.



ATTENTION: Exposure to some chemicals can degrade the sealing properties of materials used in the relay. Periodically inspect the relay and check for any degradation.

Install an SFP Module (optional)

WARNING: When you insert or remove the small form-factor pluggable (SFP) optical transceiver while power is on, an electrical arc can occur. This could cause an explosion in hazardous location installations.

Be sure that power is removed or the area is nonhazardous before proceeding.

ATTENTION: Use only Rockwell 1783-SFP100FX, 1783-SFP100LX, 1783-SFP1GSX, or 1783-SFP1GLX SFPs.

ATTENTION: We strongly recommend that you do not install or remove the SFP module with fiber optic cables attached to it because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

IMPORTANT Installing and removing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

On switch catalog numbers that support communication over fiber optic cable, SFP modules are inserted into SFP module slots on the front of the switch. These field-replaceable modules provide the uplink optical interfaces, send (TX) and receive (RX).

You can use any combination of rugged SFP modules. Each SFP module must be of the same type as the SFP module on the other end of the cable. The cable must not exceed the stipulated cable length for reliable communications.

When you use commercial SFP modules such as CWDM and 1000BX-U/D, reduce the maximum operating temperature by 15 °C (59 °F). The minimum operating temperature is 0 °C (32 °F).

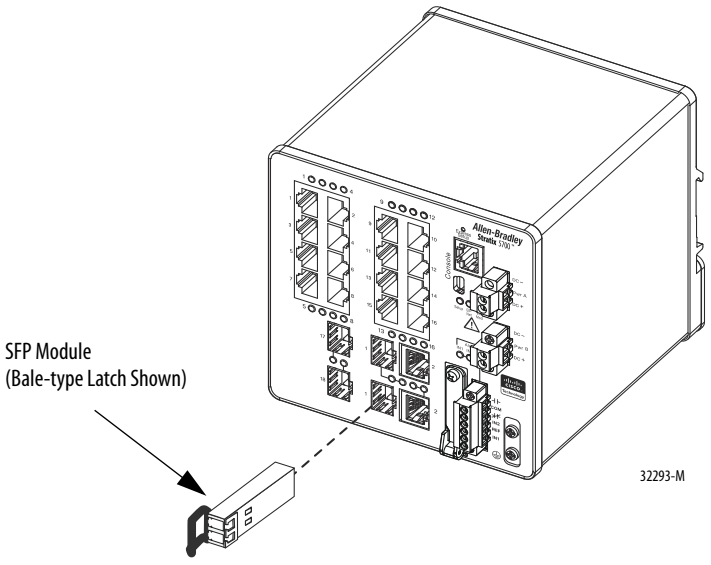
For detailed instructions on installing, removing, and cabling the SFP module, see your SFP module documentation.

To insert an SFP module into the SFP module slot, follow these steps.

1. Attach an ESD-preventive wrist strap to your wrist and to a grounded bare metal surface.
2. Grasp both sides of the SFP module and align the module sideways in front of the slot opening.

> **ATTENTION:** If the SFP module cannot be fully inserted, stop! Do not force the module into the slot. Rotate the SFP module 180° and try again.

3. Insert the SFP module into the slot as shown in the following figure until you feel the connector on the module snap into place in the rear of the slot.



4. Remove the dust plugs from the SFP module optical ports, store them for later use.

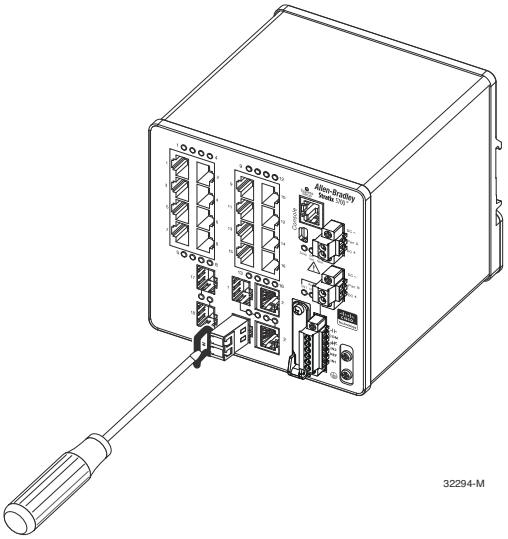
> **IMPORTANT** Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable.
>
> The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Remove SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle, follow these steps.

1. Attach an ESD-preventive wrist strap to your wrist and to a grounded bare metal surface.
2. Disconnect the fiber LC connector from the SFP module.
3. Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.
4. Unlock and remove the SFP module.

   If the module has a bale-clasp latch, swing the bale toward you and pull it gently to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.



5. Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.
6. Place the removed SFP module in an antistatic bag or other protective environment.

Wire the External Alarms

The switch has two alarm input and one Form C (single-pole, double-throw) alarm output relay circuits for external alarms. The input alarm relay circuits are designed to sense if the alarm input is open or closed relative to the alarm input reference pin. The output alarm relay circuit has a single Form C relay, with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm relay as either normally energized or normally de-energized by using the CLI.

Refer to Appendix C for an alarm wiring example.

Alarm signals are connected to the switch through the 6-way alarm relay connector. Three connections are dedicated to the two alarm input circuits:

- Alarm input 1 (IN1)
- Alarm input 2 (IN2)
- Isolated reference ground

An alarm input and the reference ground wiring connection are required to complete a single input alarm circuit. You must provide either an NO or an NC dry contact to complete the alarm circuit between reference ground and IN1 or IN2.

ATTENTION: Do not apply an external voltage source to either the IN1 or IN2 alarm inputs. Limit alarm output wiring to 48 V DC, 0.5 A.

The three remaining connections for the Form C output alarm circuit are as follows:

- NO output
- NC output
- common

An alarm output and the common wiring connection are required to complete a single output alarm circuit. The Form C output alarm relay provides one NO and one NC dry contact.

ATTENTION: Wire connections to the power and relay connector, must be UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

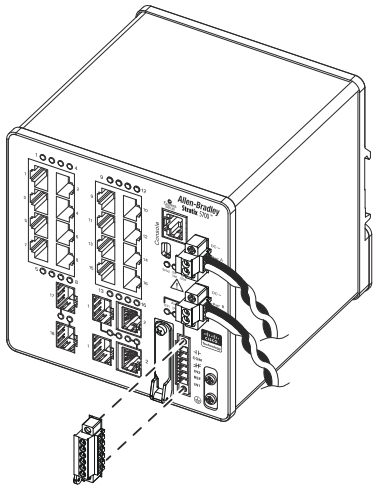
The labels for the alarm relay connector are on the switch panel.

Table 1 - Alarm Relay Connector Labels

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

To wire the switch to an external alarm device, follow these steps.

1. Loosen the captive screws that hold the alarm relay connector on the switch, and remove the connector from the switch chassis.



32287-M

2. Measure two strands of twisted-pair wire (18...20 AWG) long enough to connect to the external alarm device.

   Choose between setting up an external alarm input or output circuit.

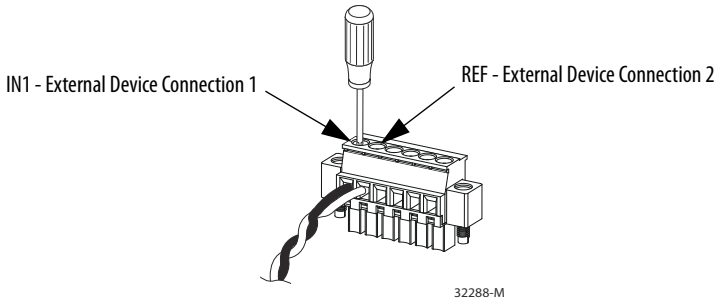
3. Use a wire stripper to remove the casing from both ends of each wire to 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.).

   Do not strip more than 6.8 mm (0.27 in.) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the alarm relay connector after installation.

4. Insert the exposed wires for the external alarm device into the connections based on an alarm input or output circuit setup. See Table 1 on page 50.

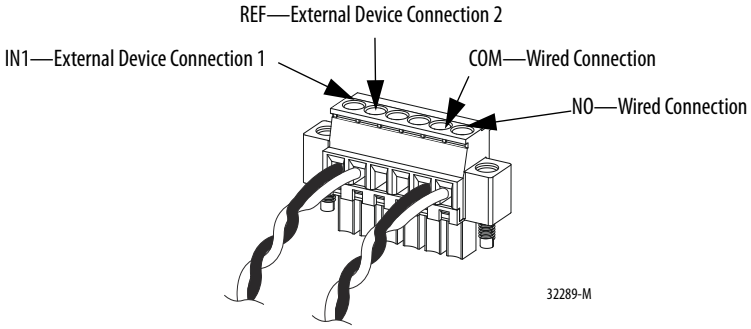
5. Use a ratcheting torque flathead screwdriver to torque the alarm relay connector captive screw (above the installed wire leads) to 0.23 N•m (2.0 lb•in).

   Do not exceed the recommended torque.



6. Repeat the above procedure to insert the input and output wires of one additional external alarm device into the alarm relay connector.

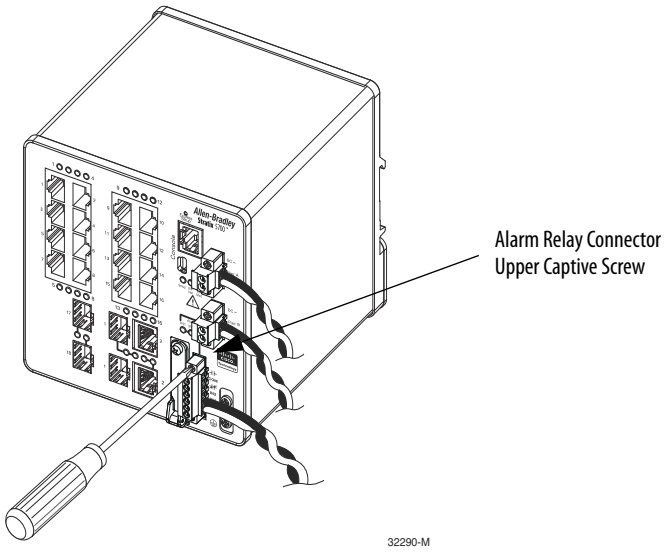
   The following figure shows the completed wiring for two external alarm devices. The first alarm device circuit is wired as an alarm relay input circuit—the IN1 and REF connections complete the circuit. The second alarm device circuit is wired as an alarm relay output circuit by using the normally open side of the form C relay contacts. The NO and COM connections complete the circuit.



Attach the Alarm Relay Connector to the Switch

To attach the alarm relay connector to the front panel of the switch, follow these steps.

1. Insert the alarm relay connector into the receptacle on the switch front panel.
2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the alarm relay connector.



Connect to 10/100 and 10/100/1000 Ports

The switch 10/100/1000 ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no linkage.

The Auto-MDIX feature is enabled by default. Unless this feature is disabled, you can use either straight-through or crossover cables to connect to other devices on the network.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

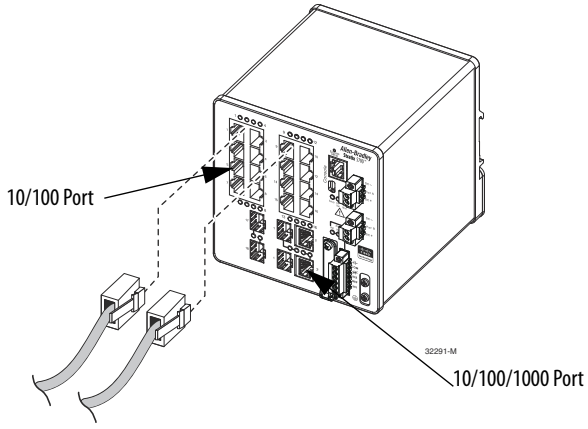
- Let the ports autonegotiate both speed and duplex
- Set the port speed and duplex parameters on both ends of the connection

Connect to 10BASE-T, 100BASE-TX, or 1000BASE-T Ports

To connect to 10BASE-T, 100BASE-TX, or 1000BASE-T ports, follow these steps.

ATTENTION: To prevent electrostatic-discharge (ESD) damage, follow recommended board and component handling procedures.

1. Choose one of these options to connect a device:
   - When connecting to workstations, servers, and routers, connect a straight-through cable to an RJ45 connector on the front panel.
   - When connecting to 1000BASE-T-compatible devices, use a twisted four-pair, Category 5e or higher cable.



2. Connect the other end of the cable to an RJ45 connector on the other device.

   The Port status indicator turns on when both the switch and the connected device have an established link.

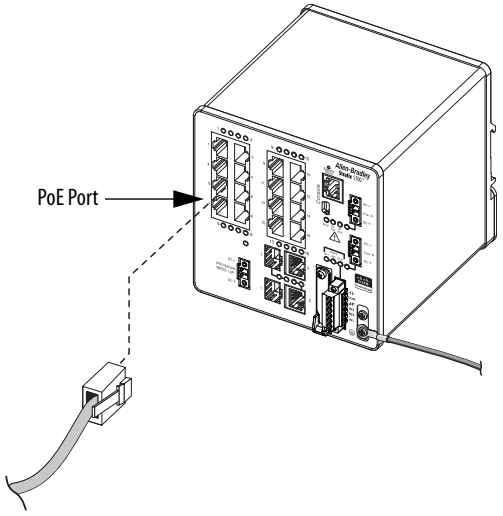
   The Port status indicator is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This can take up to 30 seconds, and then the Port status indicator turns green.

   The following conditions can prevent the Port status indicator from turning On:
   - The device at the other end is not turned On.
   - A problem exists with a cable or the adapter installed in the attached device.
3. Reconfigure and restart the connected device if necessary.
4. Repeat this procedure to connect each device.

Connect to PoE Ports

Switches with PoE ports require a separate power supply. For power supply requirements based on your application, refer to page 44.

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an RJ45 connector into the PoE port.



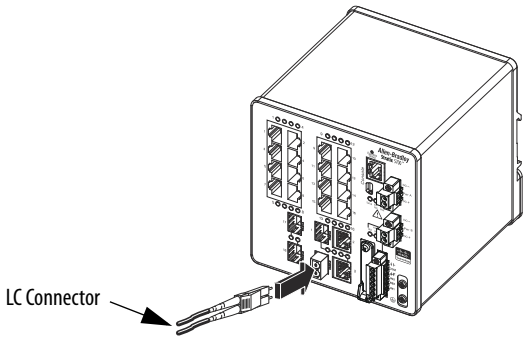
2. Insert the other cable end into an RJ45 connector on the other PoE powered device.

Connect to SFP Modules

To connect a fiber-optic cable to an SFP module, follow these steps.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

1. Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.
2. Insert one end of the fiber-optic cable into the SFP module port.



3. Insert the other cable end into a fiber-optic receptacle on a target device.
4. Observe the port status indicator:
   - The status indicator turns amber while the SFP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port status indicator turns green.
   - The status indicator turns green when the switch and the target device have an established link.
   - The status indicator turns off if the target device is not turned on or there is a problem with the cable or the adapter installed in the target device.

   If necessary, reconfigure and restart the switch or the target device.

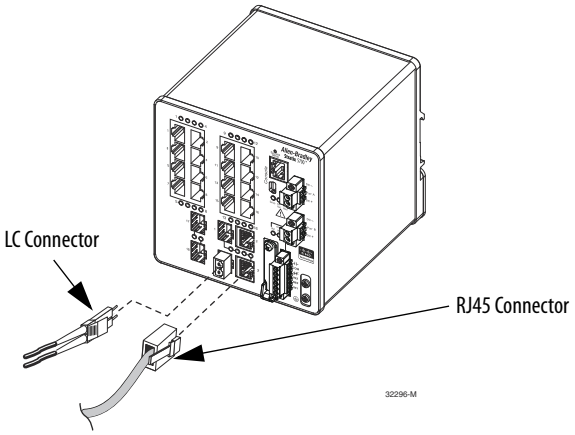
Connect to a Dual-purpose Port

A dual-purpose port is a single port with two interfaces, one for an RJ45 cable and another for an approved SFP module. Only one interface can be active at a time. If both interfaces are connected, the SFP module has priority.

ATTENTION: Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

To connect to a dual-purpose port, follow these steps.

1. Connect an RJ45 connector to the 10/100/1000 port, or install an SFP module into the SFP module slot, and connect a cable to the SFP module port.



2. Connect the other end of the cable to the other device.

   By default, the switch detects whether an RJ45 connector or SFP module is connected to a dual-purpose port and configures the port accordingly. You can change this setting and configure the port to recognize only an RJ45 connector or only an SFP module by using the media type interface configuration command. For more information, refer to the appropriate documentation at http://www.Cisco.com.

ArmorStratix 5700 Switch Installation

ATTENTION: Environment and Enclosure

This equipment is intended for use in overvoltage Category II applications (as defined in IEC 60664-1), at altitudes up to 2000 m (6562 ft) without derating.

This equipment is not intended for use in residential environments and may not provide adequate protection to radio communication services in such environments.

This equipment is supplied as enclosed equipment. It should not require additional system enclosure when used in locations consistent with the enclosure type ratings stated in the Specifications section of this publication. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings, beyond what this product provides, that are required to comply with certain product safety certifications.

In addition to this publication, see the following:

- Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional installation requirements
- NEMA Standard 250 and IEC 60529, as applicable, for explanations of the degrees of protection provided by enclosures

Installation Guidelines

ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment:

- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.

ATTENTION: Make sure all connectors and caps are securely tightened to properly seal the connections against leaks and maintain IP enclosure type requirements.

ATTENTION: The console ports are intended for temporary local programming purposes only and not intended for permanent connection.

The console port cables are not to exceed 3.0 m (9.84 ft) and must not contain hubs.

When determining where to place the switch, observe these guidelines:

- Airflow around the switch is unrestricted. To prevent the switch from overheating, observe the following minimum clearances:
  - Top and bottom: 50.8 mm (2.0 in.)
  - Sides: 50.8 mm (2.0 in.)
  - Front: 50.8 mm (2.0 in.)
- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 100 m (328 ft).
- The copper cable length from a switch to an attached device cannot exceed the distance specified in Appendix C.
- For maximum noise immunity, X-code shielded cables must be used on M12 uplink ports. For recommended M12 media, refer to http://ab.rockwellautomation.com/Connection-Devices/EtherNet-Media.
- Temperature surrounding the unit does not exceed 60 °C (140 °F).
- Clearance to front and rear panels meets these conditions:
  - Front-panel status indicators can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm relay connector are within reach of the connection to the DC power source.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Connect the unit to only an IP67-rated power supply. Rockwell Automation offers a Bulletin 1607 IP67-rated power supply to provide 24V DC power to the switch.

ATTENTION: Do not wire more than 1 conductor on any single terminal.

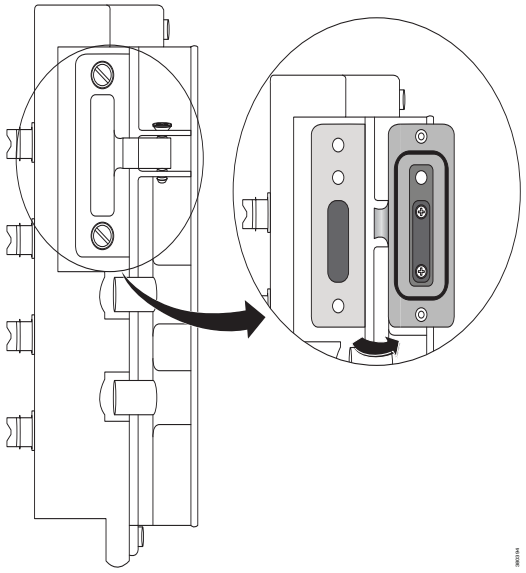
Install or Remove the SD Card (optional)

The switch supports a Secure Digital (SD) memory card to store firmware and the startup configuration. This storage makes it possible to replace a switch without reconfiguring the replacement switch.

The SD memory card cover protects the card against shock and vibration by holding the card in place. The cover is hinged and secured with captive screws. The slot for the SD memory card is located on the side of the switch.

To install or replace the SD card, follow these steps.

1. On the side of the switch, loosen the captive screws until they are free.



2. Install or remove the card:
   - To install the card, slide it into the slot, and press on it until it clicks in place. The card is keyed so that you cannot insert it the wrong way.
   - To remove the card, push it in until it releases for it to pop out. Place it in an antistatic bag to protect it from static discharge.
3. Close the guard door and fasten the captive screws to 1.8...2.2N•m (15.93...19.47 lb •in) to maintain IP67 compliance.

Verify Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up.

The time required for the switch to start up is directly related to your switch configuration. Start time is negatively affected by such things as the following:

- Spanning Tree Learning mode
- Number of files or images in onboard flash memory

To test the switch, follow these steps.

1. Power on the switch.

   To apply power to a switch that is directly connected to a DC power source, locate the circuit breaker on the panel board that services the DC circuit, and switch the circuit breaker to the ON position.

2. Verify the start-up sequence.

   When you power on the switch, it automatically begins a start-up fast routine. The System status indicator blinks green as the IOS software image loads. If the routine fails, the System status indicator turns red.

   IMPORTANT Start-up failures are usually fatal to the switch. Contact your Rockwell Automation representative immediately if your switch does not complete the start sequence successfully.

   IMPORTANT You can disable boot fast and run the Power-on Self Test (POST) by using the IOS CLI. See the appropriate documentation at http://www.Cisco.com for more information.

3. After successfully running this test, do the following:
   a. Turn off power to the switch.
   b. Disconnect the cables.
   c. Decide where you want to install the switch

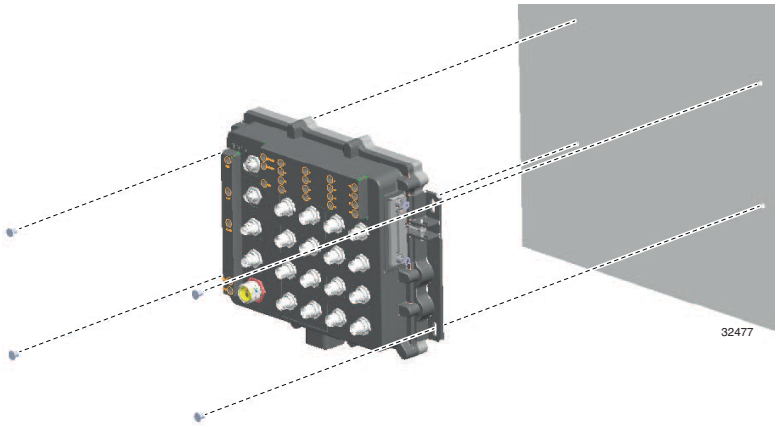
Mount the Switch

ATTENTION: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

To mount the switch, follow these steps.

1. Position the rear panel of the switch against the wall or a panel in the desired location.
2. Place a number-10 screw that you provide through each mounting ear, and screw them into the wall.



Ground the Switch

ATTENTION: This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

This equipment is intended to be grounded to comply with emission and immunity requirements. Make sure that the switch functional ground lug is connected to earth ground during normal use.

ATTENTION: To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions and use a suitable ring terminal lug, such as Thomas & Bett part number 10RCR or equivalent.

Use at least 4 mm^2 (12 AWG) wire to connect to the external grounding screw.

The ground lug is not supplied with the switch. You can use one of the these options:

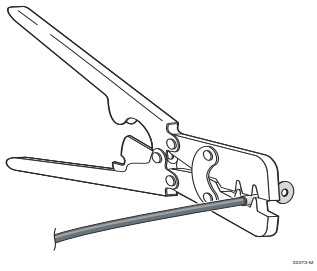
- Single ring terminal
- Two single ring terminals

To ground the switch to earth ground, follow these steps. Be sure to follow any grounding requirements at your site.

1. Use a Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the front panel of the switch.

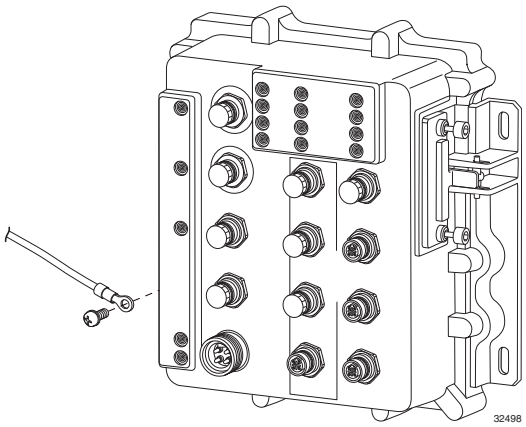
   Store the ground screw for later use.
2. Use the manufacturer's guidelines to determine the wire length to be stripped.
3. Insert the ground wire into the ring terminal lug and use a crimping tool to crimp the terminal to the wire.

   If you are using two ring terminals, repeat this action for the second ring terminal.



4. Slide the ground screw through the terminal.

5. Insert the ground screw into the functional ground screw opening on the front panel.



6. Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal lugs to the switch front panel to 0.4 N•m (3.5 lb•in).

   Do not exceed the recommended torque.

7. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

Connect the Switch to a DC Power Source

You must supply a power solution for the device. An IP67-rated cordset or patchcord with a female-end, 4-pin mini connector is required to provide power to the switch. Rockwell Automation offers a Bulletin 1607 IP67-rated power supply to provide 24V DC power to the switch. Ethernet communication and control power cables are available separately.

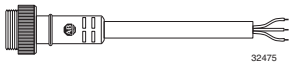
Power over Ethernet

For switches with Power over Ethernet (PoE) capability, PoE power is drawn from the single power connection. There is no separate power input for PoE.

Switch Configuration	Required Power Input	Power Supplied per Port
PoE	44-57V	15.4 W, max
PoE+	50-57V	30 W, max
Non-PoE	9.6…60V	Not applicable

Power Cables and Cordsets

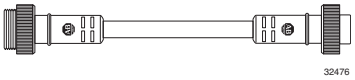
Cordsets



No. of Pins	Assembly Rating	Straight Male	Right Angle Male
4	600V, 10 A	889N-M4AFC(1)F	889N-E4AFC(1)F

(1) Replace (1) with 6 (6 ft), 12 (12 ft), or 20 (20 ft) for standard cable lengths.

Patchcords



No. of Pins	Assembly Rating	Straight Female, Straight Male	Straight Female, Right Angle Male	Right Angle Female, Straight Male	Right Angle Female, Right Angle Male
4	600V, 10 A	889N-F4AFNM-(1)	889N-F4AFNE-(1)	889N-R4AFNM-(1)	889N-R4AFNE-(1)

(1) Replace (1) with 1 (1 m), 2 (2 m), 5 (5 m), and 10 (10 m) for standard cable lengths.

Connect the DC power to the switch through the front panel connector.

Wire External Alarms

Some switch models have the following for external alarms:

- One input alarm relay circuit to sense whether the alarm input is open or closed relative to the alarm input reference pin.
- One output alarm relay circuit with a single Form C (single-pole, double-throw) relay with one normally open (NO) and one normally closed (NC) contact. You can configure the output alarm as either normally energized or normally de-energized by using the CLI.

Refer to Appendix C for an alarm wiring example.

Alarm signals are connected to the switch through the 6-way alarm relay connector. Three connections are dedicated to the alarm input.

An alarm input and the reference ground wiring connection are required to complete a single input alarm circuit. You must provide either an NO or an NC dry contact to complete the alarm circuit between reference ground and the alarm input.

The three remaining connections for the Form C output alarm circuit are as follows:

- NO output
- NC output
- common

An alarm output and the common wiring connection are required to complete a single output alarm circuit. The Form C output alarm relay provides one NO and one NC dry contact.

Use M12 A-coded cable to connect to the alarm connector on the switch. Recommended torque is 0.5...0.8 N•m (4.43... 7.08 lb•in. The recommended cable part number from Molex is 1200650523. One end of the cable has M12 A-coded connector and the other end is open.

The labels for the alarm relay connector are on the switch panel.

Table 2 - Alarm Relay Connector Labels

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

ATTENTION: The input voltage source of the alarm output relay circuit must be an isolated source and limited to less than or equal to 24 VDC, 1.0 A or 48 VDC, 0.5 A.

Connect to 10/100 and 10/100/1000 Ports

The switch 10/100 and 10/100/1000 ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no linkage.

The Auto-MDIX feature is enabled by default. Unless this feature is disabled, you can use either straight-through or crossover cables to connect to other devices on the network.

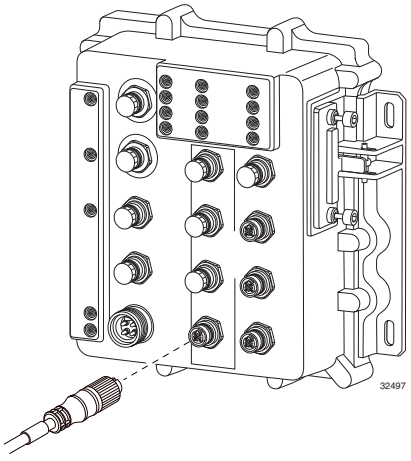
To maximize performance, choose one of these methods for configuring the Ethernet ports:

- Let the ports autonegotiate both speed and duplex
- Set the port speed and duplex parameters on both ends of the connection

Connect to PoE Ports

For power supply requirements based on your application, refer to page 64.

1. Insert a straight-through, twisted four-pair, Category 5e or better cable with an M12 connector into the PoE port.



2. Insert the other cable end into an M12 connector on the other PoE powered device.

Set Up the Switch Initially with Express Setup

When you first set up the switch, use Express Setup to enter the initial IP address. Doing this enables the switch to be used as a managed switch. You can then access the switch through the IP address for additional configuration.

IMPORTANT Do not run Express Setup with an SD card inserted in the switch.

You need this equipment to set up the switch:

- A computer with Windows 2000, Windows XP, Windows 2003, or Windows Vista operating system installed
- A supported web browser (Internet Explorer 9.0, 10.0, and 11.0, or Firefox 25, 26) with JavaScript enabled
- A straight-through or crossover Category 5 Ethernet cable to connect a computer to the switch

  or

  For ArmorStratix 5700 switches, an M12-to-RJ45 patchcord, such as Allen-Bradley catalog number 1585D-M4TBJM-2, to connect a computer to the switch
- For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches:
  - A Gigabit copper SFP module, such as Cisco model number GLC-T

    or
  - A Gigabit fiber-to-Ethernet media converter

Do the following to configure your computer:

- Disable any wireless interface running on your personal computer.
- Disable other networks in your system.
- Set your computer to automatically determine its IP address (DHCP) versus statically configured.
- Disable any static DNS servers.
- Disable browser proxy settings.

Typically, browser settings are in Tools > Internet Options > Connections > LAN Settings.

To run Express Setup, follow these steps.

1. Make sure that at least one switch Ethernet port is available for Express Setup.

   IMPORTANT For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, you must use port Gi1/1 for Express Setup. Do not use the console port.

   During Express Setup, the switch acts as a DHCP server. If your personal computer has a static IP address, change your personal computer settings before you begin to temporarily use DHCP.

2. Apply power to the switch.

   When the switch powers on, it begins its power on sequence. The power on sequence takes approximately 60 seconds to complete.

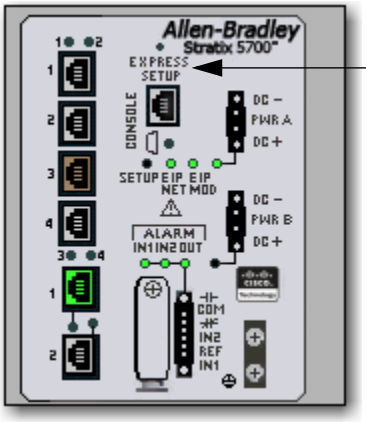
3. Make sure that the power on sequence has completed by verifying that the EIP Mod and Setup status indicators are flashing green.

   If the switch fails the power on sequence, the EIP Mod status indicator turns red.

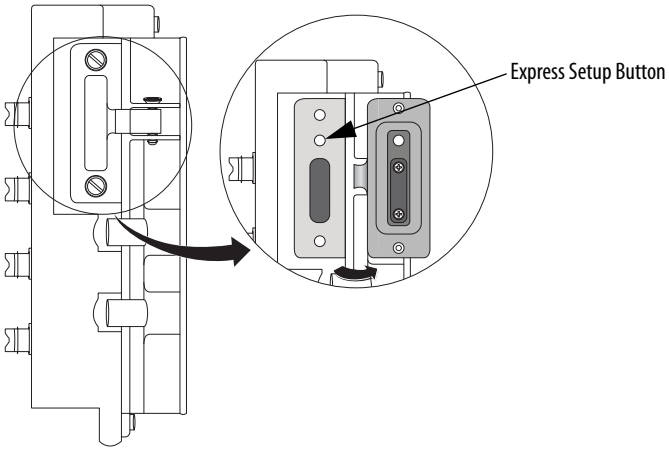
4. Press and release the Express Setup button. Wait for a few seconds until the status indicator on one of the unconnected switch ports flashes green.

   This button is recessed 16 mm (0.63 in.) behind the panel. Use a small tool, such as a paper clip, to reach the button.

Stratix 5700



ArmorStratix 5700



5. Connect a Category 5 Ethernet cable (not provided) from the flashing switch port to the Ethernet port on a computer.

   If you wait too long to connect the cable, the Setup status indicator turns off.

   or

   For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, do one of the following:

   - Insert a copper SFP module into port Gi1/1, and then connect a Category 5 Ethernet cable from the SFP module to the Ethernet port on a computer.
   - Use a fiber-to-Ethernet media converter to connect port Gi1/1 to the Ethernet port on a computer.

   IMPORTANT Port Gi1/1 does not flash during setup, but must be used to connect 1783-BMS4S2SGL or 1783-BMS4S2SGA switches to a computer.

6. Start an Internet browser session on the computer and navigate to http://169.254.0.1.

   If you have a home page configured, the switch configuration loads instead of your normal home page.

   The switch prompts you for the default switch user name and password.

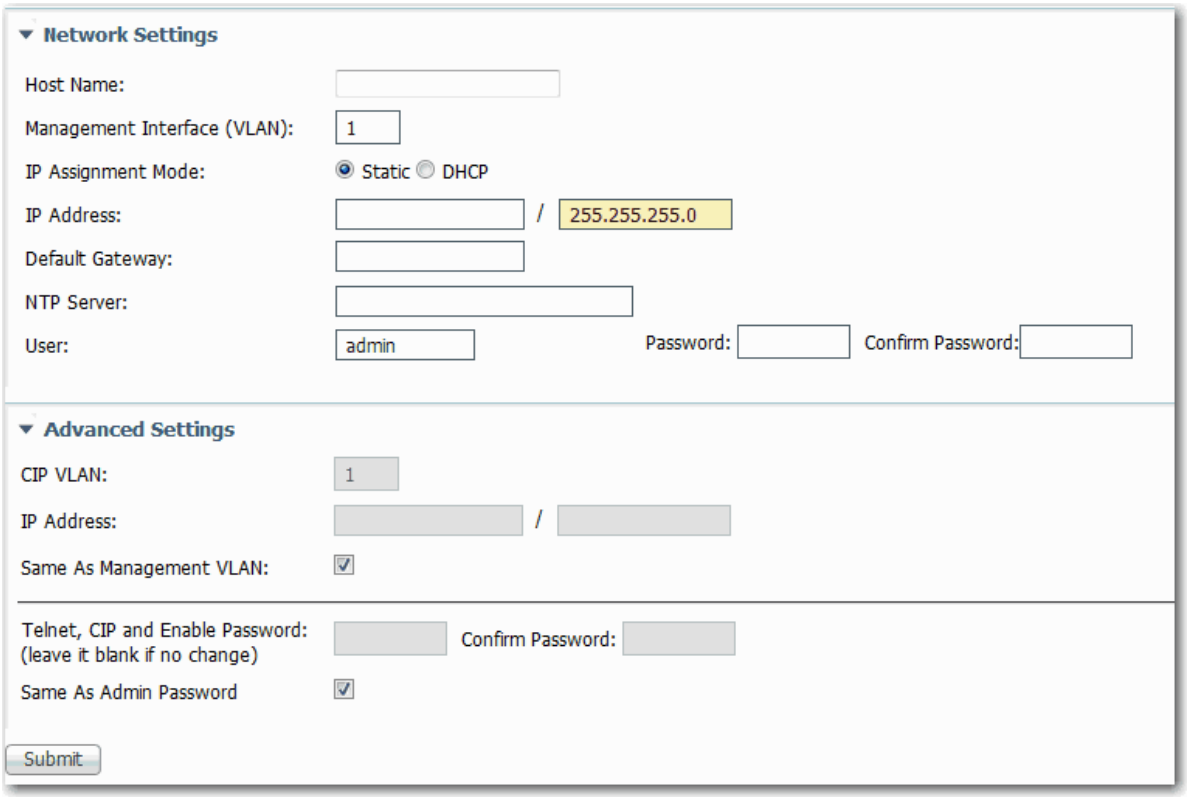
7. Leave the user name blank and enter the default switch password: **switch**.

   IMPORTANT In some scenarios, the switch requires you to enter the switch password multiple times before it accepts the password.

8. If the Express Setup window does not appear, do the following:
   - Enter the URL of a well-known website in your browser to be sure the browser is working correctly. Your browser then automatically redirects to the Express Setup web page.
   - Verify that any proxy settings or pop-up blockers are disabled on your browser.
   - Verify that any wireless interface is disabled on the computer.

9. Complete the fields.

   To view fields for Common Industrial Protocol (CIP), you must click Advanced Settings.



Field	Description
	Network Settings
Host Name	The name of the device.
Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch is managed. Choose an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1 . . . 1001. Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network at all times.
IP Assignment Mode	The IP Assignment mode determines whether the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you click Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you click DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, be sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server automatically assigns to other devices. This prevents IP address conflicts between the switch and another device.
IP Address	The IP address and associated subnet mask are unique identifiers for the switch in a network: • The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 . . . 255. • The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same.
Default Gateway (optional)	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate with each other.
NTP Server	The IP address of the Network Time Protocol (NTP) server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
User	Enter the user name.
Password, Confirm Password	The password for the switch can have up to 63 alphanumeric characters, can start with a number, is case-sensitive, and can have embedded spaces. The password cannot be a single digit, it cannot contain a ? or a tab, and it does not allow spaces at the beginning or the end. The default is **switch**. To complete initial setup, you must change the password from the default password, **switch**. This password is also used as the Control Industrial Protocol (CIP) security password. We recommend that you provide a password to the switch to secure access to the device manager.
	Advanced Settings
CIP VLAN	The VLAN on which Common Industrial Protocol (CIP) is enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on this device.
IP Address	The IP address and subnet mask for the CPI VLAN if the CIP VLAN is different from the management VLAN. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 . . . 255. Make sure that the IP address that you assign to this device is not being used by another device in your network.
Same As Management VLAN	Indicates whether the settings for the CIP VLAN are the same as the management VLAN.
Telnet, CIP and Enable Password (optional), Confirm Password	The password used for Telnet and CIP security.
Same As Admin Password	Sets the password used for Telnet and CIP security to the same user password specified under Network Settings.

10. Click Submit.

    The switch initializes its configuration for typical industrial EtherNet/IP applications. The switch then redirects you to the logon page for the Device Manager Web interface. You can continue to launch the Device Manager Web interface for further configuration or exit the application.

11. Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network.

    IMPORTANT For 1783-BMS4S2SGL or 1783-BMS4S2SGA switches, make sure DC power is disconnected prior to disconnecting Ethernet cables.

12. After you complete Express Setup, refresh the computer IP address:
    - For a dynamically-assigned IP address, disconnect the computer from the switch and reconnect the computer to the network. The network DHCP server assigns a new IP address to the computer.
    - For a statically-assigned IP address, change it to the previously configured IP address.

Notes:

Switch Software Features

Topic	Page
Port Numbering	76
Global Macro	82
Smartports	83
Power over Ethernet (PoE)	85
VLANs	90
IGMP Snooping with Querier	93
Spanning Tree Protocol	94
Port Thresholds	95
Port Security	97
EtherChannels	98
DHCP Persistence	100
CIP Sync Time Synchronization (Precision Time Protocol)	100
Network Address Translation (NAT)	101
Resilient Ethernet Protocol	107
SNMP	111
Port Mirroring	113
Routing	113
SD Card Synchronization	114
Alarms	114
Cryptographic IOS Software (optional)	114
Advanced Software Features	115

Port Numbering

The port ID consists of port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports), unit number (always 1), and port number (1-2 for Gigabit ports, 1-18 for all others, depending on catalog numbers). Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

The following table shows port numbering for the switch.

Table 3 - Port Numbering

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS06SL	6-port (4 Ethernet ports; 2 SFP slots) managed switch; lite firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SA	6-port (4 Ethernet ports; 2 SFP slots) managed switch; full firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TL	6-port (6 Ethernet ports) managed switch; lite firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TA	6-port (6 Ethernet ports) managed switch; full firmware	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SGL	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; lite firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BM06SGA	6-port (4 Ethernet ports; 2 SFP Gigabit slots) managed switch; full firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGL	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS06TGA	6-port (4 Ethernet ports; 2 Gigabit ports) managed switch; full firmware	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS10CL	10-port (8 Ethernet ports; 2 combo ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CA	10-port (8 Ethernet ports; 2 combo ports) managed switch; full firmware	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CGL	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; lite firmware	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGA	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS10CGN	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; NAT	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGP	10-port (8 Ethernet ports; 2 combo Gigabit ports) managed switch; full firmware; PTP	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS12T4E2CGNK	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware; NAT; conformal coating	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS12T4E2CGP	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; full firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS12T4E2CGL	18-port (12 Ethernet ports; 4 PoE/PoE+ ports; 2 combo Gigabit ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS20CL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CA	20-port (16 Ethernet ports; 2 SFP slots; 2 combo ports) managed switch; full firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CGL	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; lite firmware	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CGN	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; NAT	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGP	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Table 3 - Port Numbering (continued)

Cat. No.	Description	Port Numbering on Switch Labels	Port Numbering in config.text File
1783-BMS20CGPK	20-port (16 Ethernet ports; 2 SFP slots; 2 combo Gigabit ports) managed switch; full firmware; PTP; conformal coating	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Global Macro

Once you complete Express Setup, as described on page 57, the switch executes a global macro (ab-global). This macro configures the switch for typical industrial automation applications that use the EtherNet/IP protocol. This macro sets many parameters, including these major settings:

- Enable IGMP snooping and querier
- Enable CIP
- Configure QoS settings and classify CIP, PTP, and other traffic (does not apply to switches with lite firmware revisions)
- Enables alarms, SYSLOG and SNMP notifications
- Enables Rapid Spanning Tree (RSTP), BPDU Guard, BPDU Filtering, and loop guard

If you do not run Express Setup to initialize the switch, the global macro does not run. You can use the CLU to run the global macro.

Smartports

Smartports are recommended configurations for the switch ports. These configurations, referred to as port roles, optimize the switch connections and provide security, transmission quality, and reliability for traffic from the switch ports. The port roles also help prevent port misconfigurations.

TIP Use Smartport roles immediately after the initial setup of the switch to correctly configure the switch ports before they connect to devices.

Optimize Ports through Smartports Port Roles

The port roles described in Table 4 are based on the type of devices to be connected to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

Custom Smartport Roles

Stratix 5700 switches let you create and modify as many as 10 custom Smartport roles for a variety of custom applications. You can import or export custom Smartport roles only if you are using Mozilla Firefox Web browser, version 3.6 or higher. By default, the switch ports are set to the None port role.

Table 4 - Smartport Roles

Port Role	Description
Automation Device	Apply this role to ports to be connected to EtherNet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O: • Port is set to Access mode. • Port security supports only one MAC ID. • Optimize queue management for CIP traffic.
Multiport Automation Device	Apply this role to ports connected to multiport EtherNet/IP devices, such as multiport EtherNet/IP devices arranged in a linear or daisy chain topology, the 1783-ETAP module (for connection to only the device port), unmanaged switches (such as the Stratix 2000™) and managed switches with Remote Spanning Tree Protocol (RSTP) disabled: • Port is set to Access mode. • No port security. • Optimized queue management for CIP traffic.
Desktop for Automation	Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts: • Port is set to Access mode. • Portfast enabled. • Port security supports only one MAC ID. Do not apply to ports to be connected to switches, routers, or access points.
Virtual Desktop for Automation	Apply this role to ports connected to computers running virtualization software. This can be used with devices running up to two MAC addresses: • Port is set to Access mode. • Portfast is enabled. • Port security supports two MAC IDs. **IMPORTANT:** Do not apply the Virtual Desktop for Automation role to ports that are connected to switches, routers, or access points.
Switch for Automation	Apply this role to ports to be connected to other switches with Spanning Tree enabled. Port is set to Trunk mode.
Router for Automation	Apply this role to ports to be connected to routers or Layer 3 switches with routing services enabled.

Table 4 - Smartport Roles (continued)

Port Role	Description
Phone for Automation	Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer have network access through the port: • Port is set to Trunk mode. • Port security supports three MAC IDs to this port. This role prioritizes voice traffic over general data traffic to provide clear voice reception on the IP phones.
Wireless for Automation	Apply this role to ports to be connected to wireless access points. The access point can provide network access to as many as 30 wireless users.
Port Mirroring	Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 113.
None	Apply this role to ports if you do not want a specialized Smartport role on the port. This role can be used on connections to any device, including devices in the roles described above.
CS1…CS10	Custom Smartport roles. You can create a customized port role with a user-defined name. Refer to Chapter 4, Manage the Switch via the Device Manager Web Interface, for more information on creating custom Smartport roles.

Avoid Smartport Mismatches

A Smartport mismatch occurs when an attached device does not match the Smartport role applied to the switch port. Mismatches can have adverse effects on devices and your network.

Mismatches can result in the following conditions:

- Affect the behavior of the attached device
- Lower network performance (reduce the level of quality of service [QoS]) on CIP, voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial of service (DoS) attacks on the network
- Disable or shut down the port

We recommend that you always verify which Smartport role is applied to a port before attaching a device to the port or reconnecting devices.

Power over Ethernet (PoE)

Switches with PoE ports are software-configurable and provide these features:

- Support for IEEE 802.3af (PoE)-compliant devices.
- Support for IEEE 802.3at Type 2 (PoE+), which increases the available power that can be drawn by powered devices from 15.4...30 W per port.
- Automatic detection and power budgeting. The switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.
- Power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices if the switch detects that there is no power on the circuit.
- Support for Cisco Discovery Protocol (CDP) with power consumption. This features applies only when using switches with Cisco end devices. The powered Cisco end device notifies the switch of the amount of power it is consuming. The switch can supply or remove power from the PoE port.
- Support for Cisco intelligent power management. A powered Cisco end device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-powered device consuming more than 7 W to operate at its highest power mode. The powered device first starts up in Low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in High-power mode. The device changes to High-power mode only when it receives confirmation from the switch.

  Cisco intelligent power management is backward-compatible with CDP with power consumption. The module responds according to the CDP message that it receives. CDP is not supported on third-party powered devices, so the module uses the IEEE classification to determine the power usage of the device.

Powered Device Detection and Initial Power Allocation

A switch detects a powered device when a port with PoE capability is active, PoE is enabled (the default), and the connected device is not being powered by another power source.

After device detection, the switch determines the device power requirements based on its type:

- The switch classifies the detected 802.3 af/at compliant IEEE device within a power consumption class. Based on the available power in the power budget, the switch determines if a PoE port can be powered. The table below lists these levels.

  Table 5 - IEEE Power Classifications

Class	Power Supplied per Port, max
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W PoE+ devices only

- A Cisco pre-standard powered device does not provide its power requirement when the switch detects it. A port that is not configured for PoE+ allocates 15.4 W as the initial allocation for power budgeting. A port that is configured for a PoE+ switch allocates 30 W.

  The initial power allocation is the maximum amount of power that a powered device requires. The switch initially allocates this amount of power when it detects and powers the powered device. As the switch receives CDP messages from the powered device and as the powered device negotiates power levels with the module through CDP power-negotiation messages, the initial power allocation can be adjusted.

The switch monitors and tracks requests for power and grants power only when it is available. The switch tracks its power budget, which is the amount of power available on each PoE port. The switch performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to a PoE port, the switch uses CDP (if CDP is supported by the powered Cisco end device) to determine the actual power consumption requirement of the connected powered devices and adjusts the power budget accordingly. The switch processes a request and either grants or denies power. If the request is granted, the switch updates the power budget. If the request is denied, the switch verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. Powered devices can also negotiate with the module for more power.

If the switch detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and status indicators.

Power Management Modes

PoE ports support these modes:

- Auto (default)—The port automatically detects if the connected device requires power. This is the default mode. If the port discovers a connected powered device and the module has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the status indicators.

  If enough power is available for all powered devices connected to the switch, power is turned on to all devices. If there is not enough available power to accommodate all connected devices and if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

  If granting power exceeds the system power budget, the switch denies power, verifies that power to the port is turned off, generates a syslog message, and updates the status indicators. After power has been denied, the switch periodically rechecks the power budget and continues to attempt to grant the request for power.

  If a device being powered by the switch is then connected to wall power, the switch can continue to power the device. The switch can continue to report that it is still powering the device whether the device is being powered by the switch or receiving power from an AC power source.

  If a powered device is removed, the switch automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

  You can specify the maximum wattage that is allowed on the port. If the IEEE-class maximum wattage of the powered device is greater than the configured maximum value, the switch does not provide power to the port. If the switch powers a powered Cisco end device, but the powered device later requests through CDP messages more than the configured maximum value, the switch removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the switch delivers the maximum value.

- Static—The switch pre-allocates power to the port even when no powered device is connected and guarantees that power is available for the port. The switch allocates the port-configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from a powered Cisco end device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

  However, if the powered-device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that a powered Cisco end device needs more than the maximum wattage, the powered device is shut down.

  If you do not specify a wattage, the switch pre-allocates the maximum value. The switch powers the port only if it discovers a powered device. Use the static setting on a high-priority interface.

- Off—The switch disables powered-device detection and never powers the PoE port, even if an unpowered device is connected. Use this mode only when you want to make sure power is never applied to a PoE port, making the port a data-only port.

Maximum Power Allocation (cutoff power) on a PoE Port

The switch determines the cutoff power on a PoE port in this order.

1. Manually when you configure the power level to budge for the port
2. Manually when you configure the power level that limits the power allocated to the port
3. Automatically when the switch sets the power usage of the device by using the IEEE classification and LLDP power negotiation or CDP power negotiation

If you do not manually configure the cutoff-power value, the switch can automatically determine the value by using CDP power negotiation when connected to a Cisco end device. If the switch cannot determine the value by using one of these methods, it uses the default value of 15.4 W.

With PoE+, if you do not manually configure the cutoff-power value, the switch automatically determines it by using the device IEEE classification and LLDP power negotiation or CDP power negotiation with a Cisco end device. If CDP or LLDP are not enabled, the default value of 30 W is applied. However, without CDP or LLDP, the switch does not allow devices to consume more than 15.4 W of power because values from 15,400...30,000 mW are allocated based on only CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device can be in violation of the maximum current limitation and can experience a fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the switch turns on or turns off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. When you manually set the maximum power allocation, you must consider the power loss over the cable from the port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

The actual amount of power consumed by a powered device on a PoE port is the cutoff-power value plus a calibration factor of 500 mW (0.5 W). The actual cutoff value is approximate and varies from the configured value by a percentage of the configured value. For example, if the configured cutoff power is 12 W, the actual cutoff-value is 11.4 W, which is 0.05% less than the configured value.

Because the switch supports external removable power supplies for PoE/PoE+ and can configure the budget per the power supply used, the total amount of power available for the powered devices varies depending on the power supply configuration:

- If a power supply is removed and replaced by a new power supply with less power and the module does not have enough power for the powered devices, the switch denies power to the PoE ports that are in Auto mode in descending order of the port numbers. If the switch still does not have enough power, it denies power to the PoE ports in Static mode in descending order of the port numbers.

- If the new power supply supports more power than the previous one, and the switch now has more power available, the switch grants power to the PoE ports in Static mode in ascending order of the port numbers. If it still has power available, the switch then grants power to the PoE ports in Auto mode in ascending order of the port numbers.

IMPORTANT For power to be assigned accurately, the total wattage of the power supply must be manually configured via the Device Manager Web interface or CIP.

VLANs

A virtual local-area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

The switch ships with a default VLAN to which each switch port initially belongs. The switch supports a maximum of 255 VLANs, including the default VLAN.

Every VLAN is identified by its name and ID number. The default VLAN is named default. The ID can be from 1...1001 and 1005...4094, where 1 is the default ID.

You can assign switch ports to either the default VLAN or to VLANs that you have created. The default VLAN alone can be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

With custom Smartports, you can specify the type of VLAN you want to implement on that port.

The default VLAN is also the management VLAN. After the initial setup, you can create VLANs and designate any VLAN on the switch as the management VLAN. The management VLAN provides administrative access to the switch. You must assign one of the switch ports to the management VLAN. Otherwise, you do not have administrative access to the switch. Initially, all ports are assigned to the management VLAN.

You can assign all ports, regardless of their Smartport role, to the default VLAN (default).

Isolate Traffic and Users

By using VLANs, you can isolate different types of traffic, such as voice and data, to preserve the quality of the transmission and to minimize excess traffic among the logical segments. You can also use VLANs to isolate different types of users. For example, you can restrict specific data broadcasts to specific logical workgroups for security purposes, such as keeping information about employee salaries only on devices in a VLAN created for payroll-related communication.

An added benefit to using VLANs is to reduce the amount of administrative effort required to constantly examine requests to network resources.

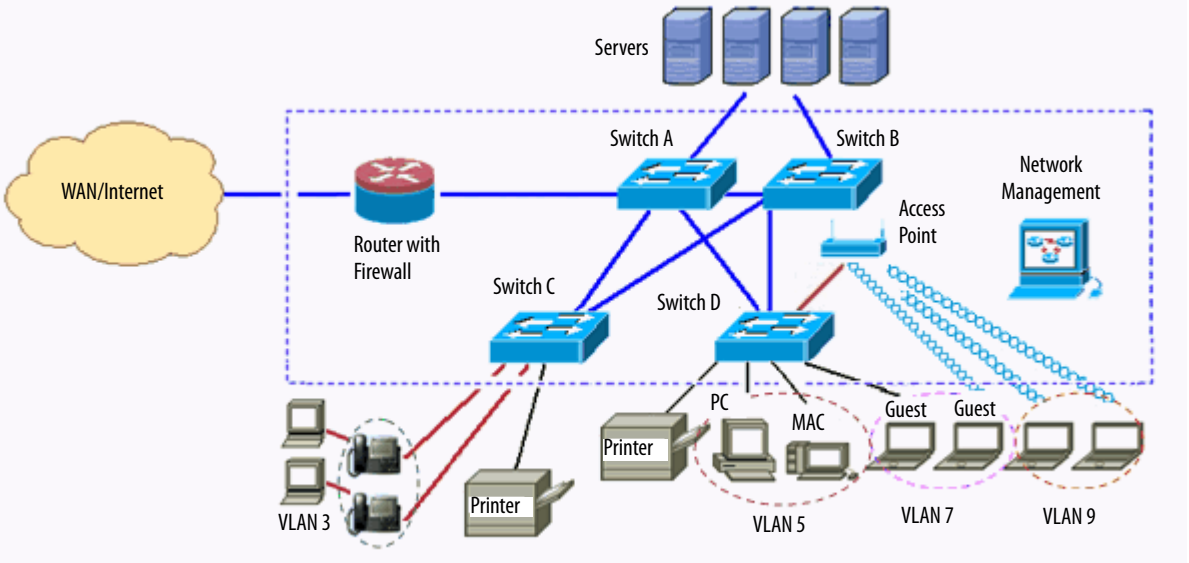
VLANs isolate parts of your network. Therefore, devices that are attached to the switch ports in the same VLAN (network users in the same VLAN) can communicate only with each other and can share the same data.

Devices attached to switch ports in different VLANs cannot communicate with each other through the switch, unless the switch is configured for routing. A Stratix 5700 switch, a router, or a Layer 3 switch must be configured to enable routing across VLANs (inter-VLAN routing), and additional security policies must be set.

If your network is also using a DHCP server, make sure that the server is accessible to the devices in all the VLANs.

The following figure is an example network that uses VLANs based on different network traffic and network users. Organizing a network around these factors helps to define the size and membership of the VLANs in the network.

Figure 1 - VLAN Example



Isolate Different Traffic Types

Isolating data traffic from delay-sensitive traffic, such as voice traffic, increases the quality of the voice transmission. In the figure above, switch ports connected to the IP phones belong to VLAN 3, a VLAN that is configured to provide Voice over IP (VoIP) services on these connections, meaning priority is given to voice traffic over regular IP data traffic. Voice traffic from the phone and IP-phone service requests to an IP PBX server have priority over traffic from the desktop devices attached to the IP phones.

To further isolate data traffic from voice traffic, the data traffic from the attached desktop devices can be assigned to a separate VLAN.

Group Users

The network shown in Figure 1 provides access to three types of network users:

- Wired employees
- Wireless employees
- Wired or wireless company visitors

Each user type requires different access levels to the company network. VLANs and security policies on a router or Layer 3 switch can enforce privileges and restrictions to different user types.

Refer to Figure 1 on page 91:

- VLAN 5 offers employee-level access to the company resources. This kind of network access requires a direct connection to the specific switch ports.
- VLAN 7 offers Internet-only access to company visitors. Visitors with wired or wireless connections to switch ports are assigned to this VLAN, which automatically restricts guest access to only the Internet.
- VLAN 9, which has one or more switch ports connected to the wireless access point, enforces security policies to identify the wireless user (for example, as employee or a guest) and to determine what the user can do on the network (for example, access only the Internet or access other network resources).

IGMP Snooping with Querier

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

256 is the default number of multicast groups supported in the switches. If you exceed 180 multicast groups, we recommend that you switch to the routing SDM template by using the CLI.

The IP multicast groups learned through IGMP snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Multicast IP addresses used by the EtherNet/IP network for I/O traffic are learned by the switch.

IGMP implementation in the switch is IGMP V2. This version is backward-compatible with switches running IGMP V1. The switch has a built-in querier function, and the global macro enables on IGMP Snooping and the querier.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations can receive duplicate messages. Switches can also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

You can choose one of these options:

- The default Rapid Spanning Tree Protocol (RSTP) (also known as Multiple Spanning Tree Protocol [MST])
- Per-VLAN Spanning Tree Protocol (PVST+)
- Rapid Per-VLAN Spanning Tree Protocol (RPVST+)

TIP If you are connecting the switch to a Cisco network switch, the typical default is PVST+, not RSTP. To provide compatibility, one or the other switch must be modified.

Port Thresholds

Port thresholds prevent traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. Port Thresholds do not apply to switches with lite firmware.

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing denial-of-service attacks can cause a storm.

Incoming (storm control)

Incoming port thresholds (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Port thresholds uses one of these methods to measure traffic activity:

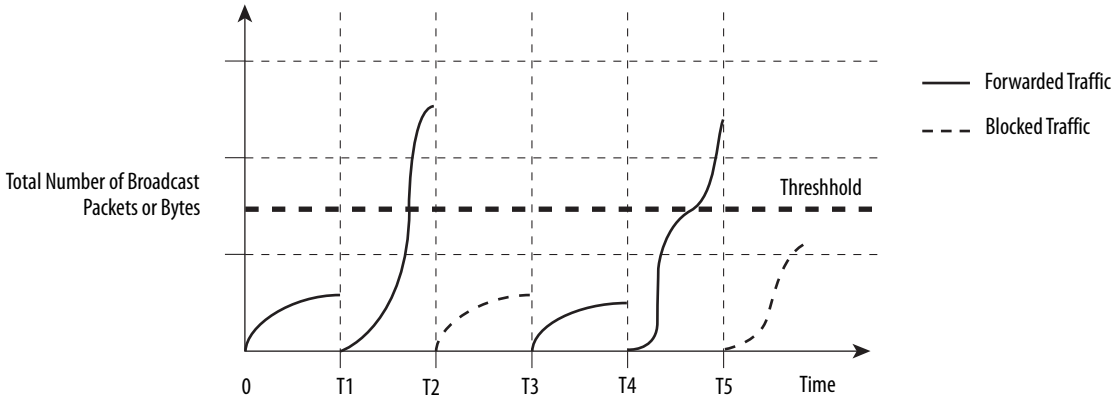
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic.
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received.
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold and then resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

IMPORTANT When the port threshold for multicast traffic is reached, all multicast traffic except network management traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

The graph shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 2 - Port Thresholds Example



The combination of the storm-control suppression level and the 1-second time interval controls the way the port thresholds algorithm works. A higher threshold enables more packets to pass through. A threshold value of 100% means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

IMPORTANT Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of port thresholds.

Outgoing (rate limiting)

Outgoing port thresholds limit the rate at which the switch communicates with a client device as a percentage of wire speed (the amount of the rate limit as a percentage of the total). Limiting bandwidth to specific users and ports helps control network congestion, enable high performance, create efficient networks, and prevent a small number of devices from monopolizing network bandwidth. It can also improve reliability by limiting maximum bandwidth to end devices that are not be capable of handling large amounts of traffic. From the Device Manager Web interface or the Logix Designer application AOP, you can enable or disable rate limiting on a per port basis.

Default Port Thresholds Configuration

By default, incoming unicast, broadcast, and multicast port thresholds are disabled. Outgoing port thresholds are also disabled.

Port Security

Stratix 5700 switches implement MAC address-based port security. A MAC address is a unique address assigned to each Ethernet-capable device. This means that the switch can enforce communications either dynamically or statically per MAC address.

With dynamic port security, a switch port communicates with a certain number of devices (MAC addresses). The port tracks only the number of devices rather than the MAC addresses of those devices. Static port security adds devices to the port security table on a per MAC address basis. With static dynamic port security, only devices with the MAC addresses in the security table are able to communicate on that port.

One or both methods can be used in the Stratix 5700 switches with Full firmware on a per-port basis. Port Security does not apply to switches with lite firmware.

Dynamic Secure MAC Address (MAC ID)

Many Smartport roles have a maximum number of MAC IDs that can use that port. For example, the Smartport role 'Automation Device' sets up the port for a maximum of one MAC ID. The MAC ID is dynamic, meaning the switch learns the first source MAC ID to use the port. Attempts by any other MAC ID to access the port are denied.

If the link becomes inactive, the switch dynamically relearns the MAC ID to be secured.

The default number of MAC IDs can be changed on the Port Security tab within the Device Manager Web interface or the Logix Designer application.

The following table shows the Smartport role and the maximum number of supported MAC IDs.

Table 6 - Maximum Number of MAC IDs per Smartport Role

Smartport Role	Number of MAC IDs (max)
Automation Device	1
Desktop for Automation	1
Switch for Automation	Not restricted
Router for Automation	Not restricted
Phone for Automation	3
Wireless for Automation	Not restricted
Multiport Automation Devices	Not restricted
Virtual Desktop for Automation	2
Port Mirroring	Not restricted
None	Not restricted

Static Secure MAC Address (MAC ID)

The other method of limiting MAC IDs is to statically configure one or more MAC IDs for a port by defining them via port security on the Device Manager Web interface. These addresses become part of the saved configuration of the switch. This method provides strong security. However, if you replace any devices connected to the port, you must reconfigure the MAC IDs because the new devices have different MAC IDs than the previous devices.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses that have been configured for a port have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a violation occurs, the port goes into the Restrict mode. In this mode, packets with unknown source addresses are dropped and you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

EtherChannels

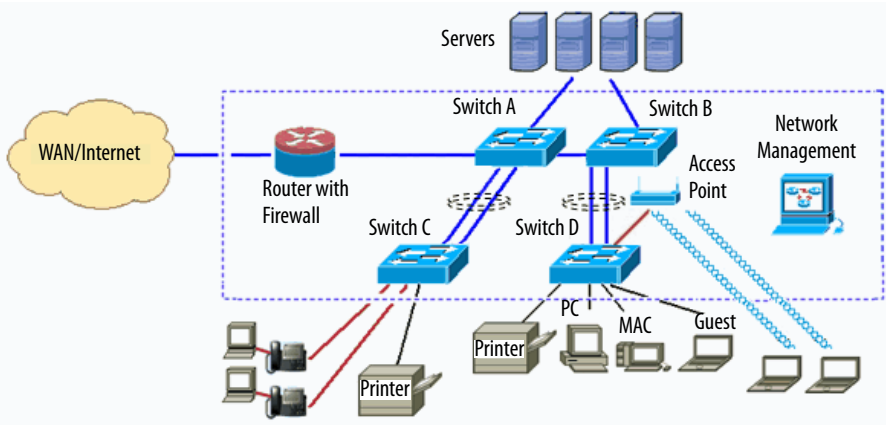
An EtherChannel (or port group) is a group of two or more Fast Ethernet or Gigabit Ethernet switch ports bundled into a single logical link, creating a higher bandwidth link between two switches.

The switch supports up to six EtherChannels. Each EtherChannel can consist of up to eight compatible, configured ethernet ports. EtherChannels do not apply to switches with lite firmware.

The following figure shows two EtherChannels. Two full-duplex 10/100/1000-Mbps ports on Switches A and C create an EtherChannel with a bandwidth of up to 4 Gbps between both switches. Similarly, two full-duplex 10/100 ports on Switches B and D create an EtherChannel with a bandwidth of up to 400 Mbps between both switches.

If one of the ports in the EtherChannel becomes unavailable, traffic is sent through the remaining ports within the EtherChannel.

Figure 3 - EtherChannel Example



You can configure an EtherChannel in one of these modes:

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- On

Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine the ports to become active. Incompatible ports are suspended. Instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

- When you configure an EtherChannel in the On mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the On mode; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

DHCP Persistence

Every device in an IP-based network must have a unique IP address. The Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. If a device leaves and then re-joins the network, the device receives the next available IP address, which can or cannot be the same address that it had before.

The switch can be set to operate as a DHCP server to provide DHCP persistence. With DHCP persistence, you can assign a specific IP address to each port to make sure that a device attached to a specific port receives the same IP address. This feature works with only a single device connected to each port configured for DHCP persistence.

IMPORTANT To make sure DHCP persistence works correctly, follow the application rules.

CIP Sync Time Synchronization (Precision Time Protocol)

The IEEE 1588 standard defines a protocol called Precision Time Protocol (PTP) that enables precise synchronization of clocks in measurement and control systems. We refer to this as CIP Sync time synchronization. The clocks are synchronized over the EtherNet/IP communication network. PTP enables systems that include clocks of various precision, resolution, and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the Grandmaster clock.

Three PTP modes are available for the switches:

- Boundary Clock
- Transparent Clock
- Forwarding (PTP is disabled when Forwarding mode is selected)

For more information on these modes, refer to the Converged Plantwide Ethernet Design and Implementation Guide, publication ENET-TD001.

The default PTP mode is Forwarding mode.

Network Address Translation (NAT)

NAT is a service that translates one IP address to another IP address via a NAT-configured switch. The switch translates the source and destination addresses within data packets as traffic passes between subnets.

This service is useful if you need to reuse IP addresses throughout a network. For example, NAT makes it possible for devices that share a single IP address on a private subnet to be segmented into multiple identical private subnets while maintaining unique identities on the public subnet.(1)

The implementation of NAT in the Stratix 5700 switch is distinct in these ways:

- One-to-one NAT—The switch uses one-to-one NAT, rather than one-to-many NAT. One-to-one NAT requires that each source address translates to one unique destination address. Unlike one-to-many NAT, multiple source addresses cannot share the same destination address.
- Layer 2 implementation—The switch's implementation of NAT operates at the Layer 2 (MAC) level. At this level, the switch can replace only IP addresses and does not act as a router.

Configuration Overview

To configure NAT, you create one or more unique NAT instances. In a typical implementation, only one instance is required. A NAT instance contains entries that define each address translation, as well as other configuration parameters.

The translations you define depend on whether traffic is routed through a Layer 3 switch or router or a Layer 2 switch:

- If traffic is routed through a Layer 3 switch or router (Figure 4), you define the following:
  - A private-to-public translation for each device on the private subnet that needs to communicate on the public subnet.
  - A gateway translation for the Layer 3 switch or router.

  You do not need to configure NAT for all devices on the private subnet. For example, you can choose to omit some devices from NAT to increase security, decrease traffic, or conserve public address space.

  IMPORTANT As a best practice, we recommend you route traffic through a Layer 3 switch or router.

- If traffic is routed through a Layer 2 switch (Figure 5), you define the following:
  - A private-to-public translation for each device on the private subnet that needs to communicate on the public subnet.
  - A public-to-private translation for each device on the public subnet that needs to communicate on the private subnet.

(1) Note that we use the terms private and public to differentiate the two networks on either side of the NAT device. This does not infer that the public network must be internet routable.

Figure 4 - Layer 3 Example

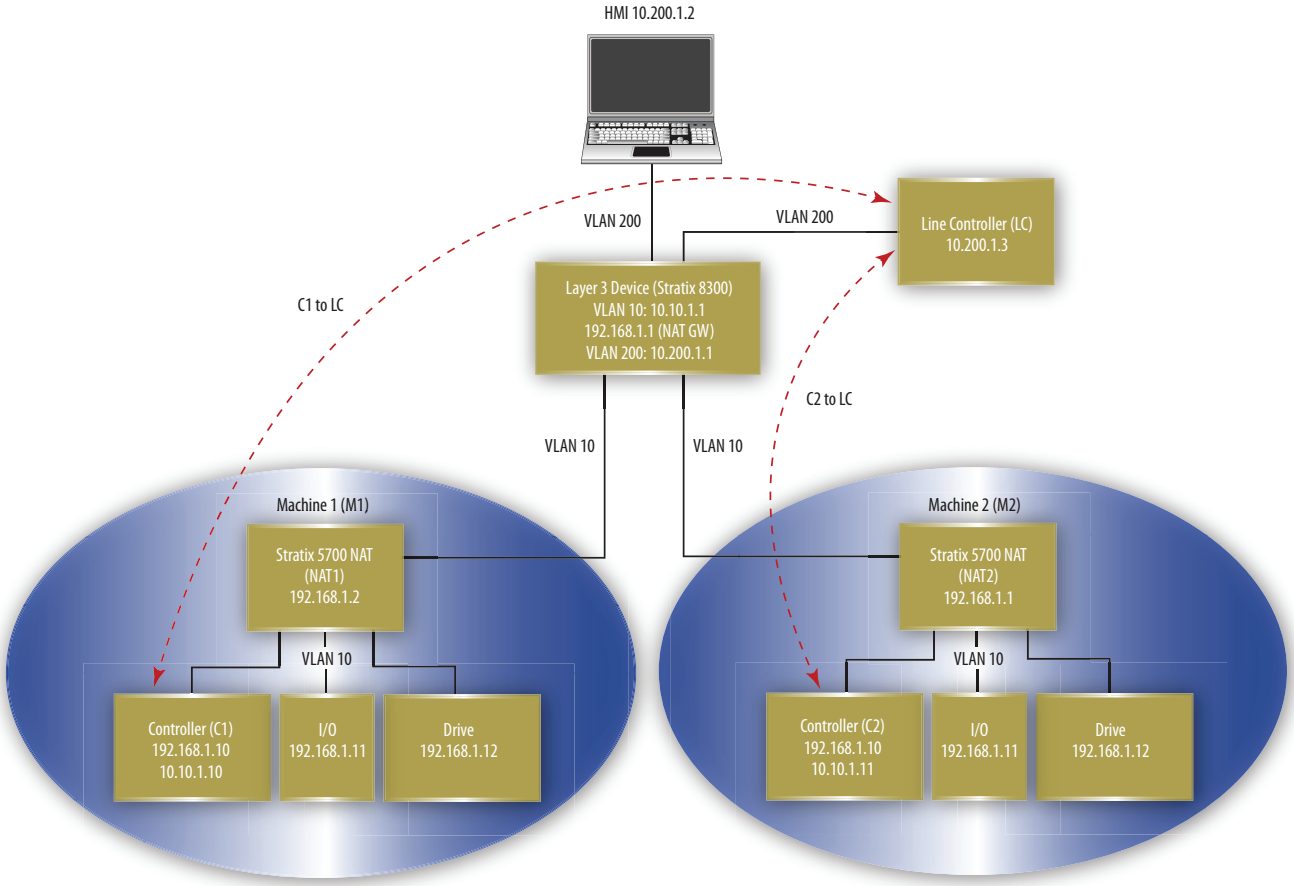
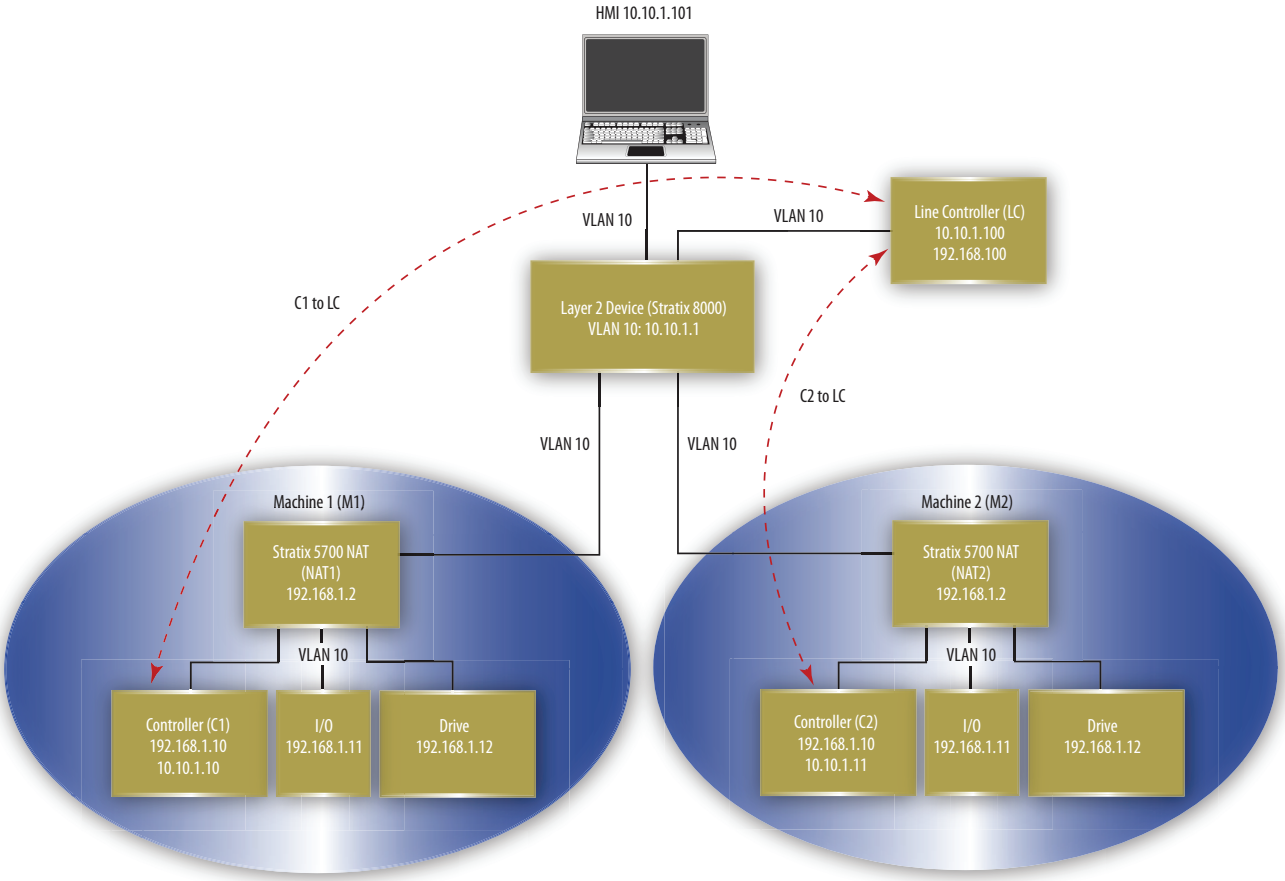


Figure 5 - Layer 2 Example



An address translation can be one of three types. The type of translation determines the number of translation entries. A switch can have a maximum of 128 translation entries.

Table 7 - Number of Translation Entries by Translation Type

Translation Type	Translation Entries	Description
Single	1	Translates a single IP address. Consists of the following: • One private IP address • One public IP address
Range	Multiple	Translates a range of IP addresses. Consists of the following: • One starting private IP address • One starting public IP address • Multiple entries based on the range you specify
Subnet	1	Translates all of the IP addresses within a subnet or portion of a subnet. Consists of the following: • One starting private IP address • One starting public IP address aligned on valid subnet boundaries • Subnet mask

EXAMPLE The following translation types count as 10 translation entries:

- Single translation for one device
- Range translation for eight devices
- Subnet translation for all the devices on the subnet

Singe and range translation types have a one-to-one relationship between translations entries and addresses to be translated. However, subnet translations have a one-to-many relationship allowing one translation entry for many addresses.

VLAN Assignments

When configuring NAT, you can assign one or more VLANs to a NAT instance. When you assign a VLAN to a NAT instance, the traffic associated with that VLAN is subject to the configuration parameters of the NAT instance. Configuration parameters include whether traffic is translated, fixed up, blocked, or passed through.

IMPORTANT Set up all Smartport roles and VLANs before creating NAT instances.

If you change a Smartport role or the native VLAN for a port associated with a NAT instance, you must reassign VLANs to the NAT instance.

When assigning VLANs to a NAT instance, consider the following:

- NAT supports both trunk ports and access ports.
- NAT does not change VLAN tags.
- You can assign a maximum of 128 VLANs to one or more instances.
- You can assign the same VLAN to multiple instances as long as the VLAN is associated with different ports. For example, you can assign VLAN 1 to both instance A and instance B as long as VLAN 1 is associated with port Gi1/1 on instance A and port Gi1/2 on instance B.
- By default, each instance is assigned to all VLANs on port Gi1/1 and no instances on port Gi1/2.

VLANs associated with a trunk port can or can not be assigned to a NAT instance:

- If a VLAN is assigned to a NAT instance, its traffic is subject to the configuration parameters of the NAT instance.
- If a VLAN is unassigned to a NAT instance, its traffic remains untranslated and is always permitted to pass through the trunk port.

Management Interface and VLANs

The management interface can be associated with a VLAN that is or is not assigned to a NAT instance:

- If its associated VLAN is assigned to a NAT instance, the management interface resides on the private subnet by default. To manage the switch from the private subnet, no additional configuration is required. To manage the switch from the public subnet, you must configure a private-to-public translation.
- If its associated VLAN is not assigned to a NAT instance, the management interface's traffic remains untranslated and is always permitted to pass through the port.

Configuration Considerations

Consider these guidelines and limitations when configuring NAT:

- A switch can translate only IPv4 addresses.
- A switch can have a maximum of 128 NAT instances, 128 NAT-associated VLANs, and 128 translation entries. A subnet translation counts as only one translation entry, but includes translations for many devices.
- You can configure NAT on one or both uplink ports of the switch.

IMPORTANT Some NAT configurations can result in greater-than-expected traffic loads on both private and public subnets. Also, unintended traffic can be visible.

NAT is not a substitute for a firewall. Make sure your configuration is performance qualified prior to use in a production environment.

Ports configured for NAT do **not** support the following across the NAT boundary due to embedded IP addresses that are not fixed up, encrypted IP addresses, or reliance on multicast traffic:

- Traffic encryption and integrity checking protocols generally incompatible with NAT, including IPsec Transport mode (1756-EN2TSC module)
- Applications that use dynamic session initiations, such as NetMeeting
- File transfer protocol (FTP)
- Microsoft Distributed Component Object Model (DCOM), which is used in Open Platform Communications (OPC)
- Multicast traffic, including applications that use multicast, such as CIP Sync (IEEE1588) and CLX redundancy

Traffic Permits and Fixups

While a NAT-configured port can translate many types of traffic, only unicast and broadcast traffic are supported. You can choose to block or pass through the following traffic types that are not handled by NAT:

- Untranslated unicast traffic
- Multicast traffic
- IGMP traffic

By default, all of the above traffic types are blocked.

Some traffic types must be fixed up to work properly with NAT because their packets contain embedded IP addresses. The switch supports fixups for these traffic types:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)

By default, fixups are enabled for both ARP and ICMP.

Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) provides an alternative to Spanning Tree Protocol (STP) to control network rings and loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, makes sure that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

REP is a segment protocol. One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (transit) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium; however, on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces. Selecting the Switch for Automation Smartport enables Layer 2 trunking. REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

These types of REP ports are selectable in the Device Manager Web interface:

- Primary—This port is a primary edge port. This port always participates in VLAN load balancing in the REP segment.
- Edge—This port is a secondary edge port. It also participates in VLAN load balancing in the REP segment.

  Edge ports are termination points of a REP segment. The user must configure two edge ports, including one primary edge port, for each REP segment. Entering edge without primary configures the port as a secondary edge port. Primary and secondary edge ports must be configured even if support of VLAN balancing is not required.
- Transit—This port is a non-edge port in the REP segment.
- No-Neighbor Primary—This port is a primary edge port connected a non-REP switch.
- No-Neighbor—This port is a secondary edge port connected to a non-REP switch.

  The no-neighbor edge ports contain all properties of regular edge ports. These ports enable the construction of a REP ring containing a switch that does not support REP protocol.
- None—This port is not part of the REP segment.

REP and STP can coexist on the same switch, but not on the same port. REP does not interact with STP. For example, if a port is configured as an REP port, STP is disabled on that port. STP bridge protocol data units (BPDUs) are not accepted on or sent from REP ports. However, adjacent REP and STP rings or domains can share a common link. This common link can be used for passing REP and STP date plane traffic, or for the STP control plane traffic.

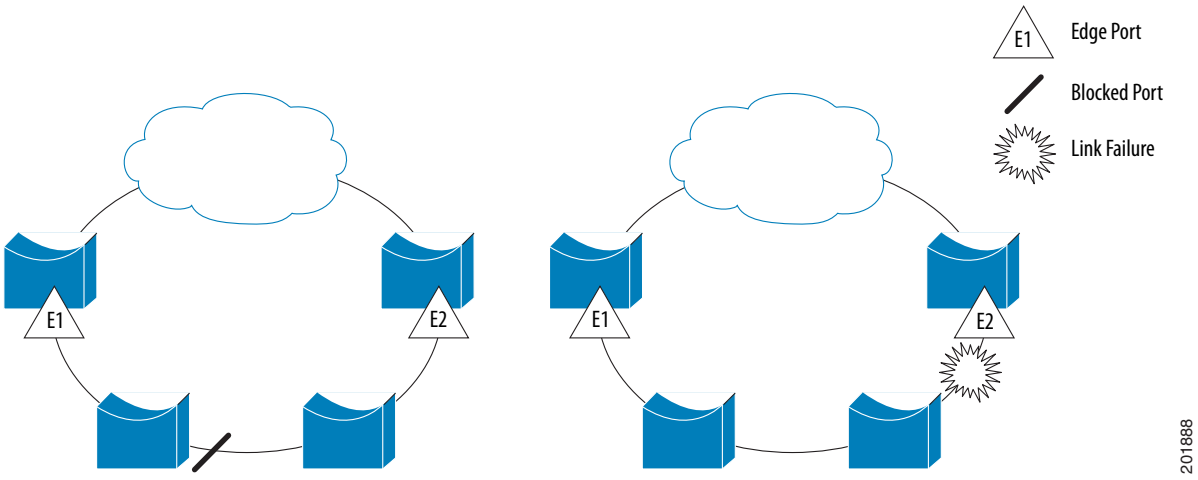
Figure 6 shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

REP Open Segment

The segment shown in Figure 6 is an open segment. There is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure causes a host to be unable to access its usual gateway, REP unblocks all ports to make sure that connectivity is available through the other gateway.

In the following example, E1 or E2 can be configured as the primary edge port.

Figure 6 - Open Segment Example

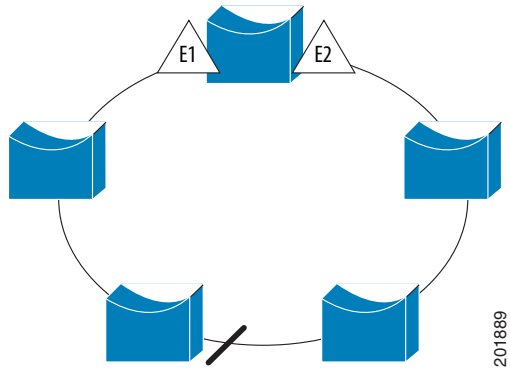


REP Ring Segment

The segment shown in Figure 7, with both edge ports on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

In the following figure, E1 or E2 can be configured as the primary edge port.

Figure 7 - Ring Segment Example



REP segments have these characteristics:

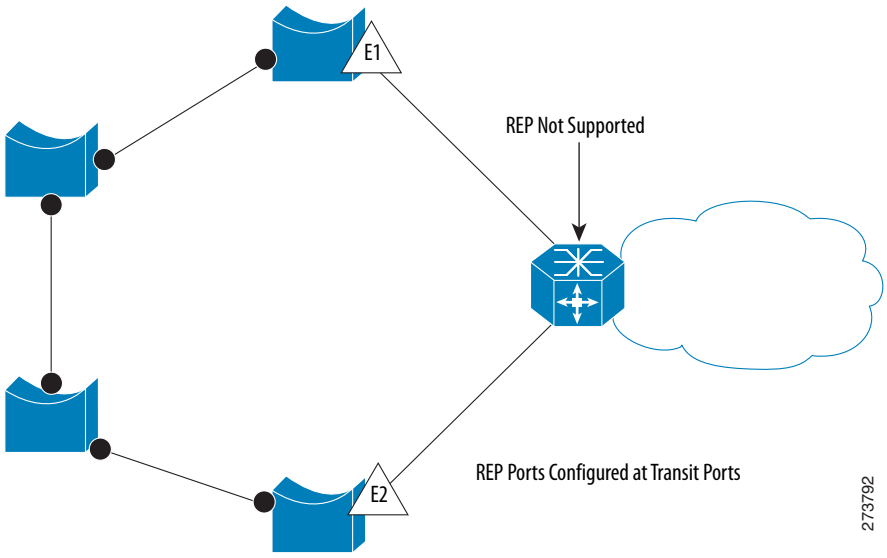
- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to support ongoing connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

Access Ring Topologies

In access ring topologies, the neighboring switch cannot support REP, as shown in Figure 8. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

In the following example, E1 or E2 can be configured as the primary no-neighbor port.

Figure 8 - Ring Topology Example



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

Configure REP in networks only with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines the neighbor port to become the alternate port and which ports forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

SNMP

The switch supports Simple Network Management Protocol (SNMP) versions 1, 2C, and 3. SNMP enables the switch to be remotely managed through other network management software. This feature is disabled by default.

SNMP is based on three concepts:

- SNMP managers (client software)
- SNMP agents (network devices)
- Management Information Base (MIB)

Refer to Supported MIBs on page 112 for the MIBs supported on the switch.

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, have an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB and to set values in the MIB. The agent and the MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Both SNMPv1 and v2C use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community strings. SNMPv1 and v2C are generally used for network monitoring without network control.

SNMPv3 provides network monitoring and control. It provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security model used by SNMPv3 is an authentication strategy that is set up for a user and the user's group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

These are some guidelines about SNMPv3 objects:

IMPORTANT SNMPv.3 is available only in the cryptographic version of the switch firmware.

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy defines which SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications that its users can receive.
- A group also defines the security model and the security level for its users.
- An SNMP view is a list of MIBs that a group can access.
- Data can be securely collected from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router configuration, can be encrypted to prevent the contents from being exposed on the network.

Supported MIBs

The Stratix 5700 switch supports the following MIBs.

Table 8 - Supported MIBs

MIB Name		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

Port Mirroring

Port mirroring is for advanced users with experience in troubleshooting traffic and protocol issues on networks. The port mirroring feature copies (or mirrors) traffic on one port to a monitoring port where the packet can be captured by a network protocol analyzer tool. Use port mirroring as a diagnostic tool or debugging feature.

Port mirroring does not affect the switching of network traffic on the monitored port. You must dedicate a monitoring port for port mirroring use. Except for traffic that is being copied for the port mirroring session, the monitoring port does not receive or forward traffic.

You can configure port mirroring by assigning the Port Mirroring Smartport role on a switch port via the Device Manager Web interface.

Routing

The switch supports these forms of routing:

- Static routing—Defines explicit paths between two devices (routers and switches). You must manually define the route information, including the destination IP address, destination subnet mask, and next hop router IP address.

- Connected routing—Enables all devices on any VLAN that use the switch to communicate with each other if they use the switch as their default gateway. Connected routing is automatically enabled if you enable static routing. To disable connected routing and prevent inter-VLAN communication, you must configure access control lists (ACLs) by using the CLI.

Enabling routing is a two-step process within the Device Manager Web interface:

1. Reallocate switch memory for routing by changing the Switch Database Management (SDM) template from the default template to the Lanbase Routing template.
2. Enable connected routing only.

   or

   Enable and configure static routing, which enables connected routing by default.

Configuration Management

The switch can store its configuration in internal memory or on an external SD card. By default, the SD card always takes precedence over internal memory. If you have a valid IOS image and configuration files on the SD card and start the switch with the SD card inserted, the switch loads the files from the SD card.

In general, the start method for the switch becomes the source for any changes you make to the configuration. For example, if you start from the SD card, any changes you make are saved to the SD card. If you start the switch from internal memory, even if you insert an SD card while starting the system, changes are saved to internal memory. To determine the start method, click the SD Sync tab from the Device Manager Web interface.

The configuration files (config.text & vlan.dat) are in human readable ASCII format. You can download the files to a computer by using one of these methods:

- FTP
- AOP
- By using a computer to read the SD card

You can also store the configuration files as part of your controller project in the Logix Designer application.

The Device Manager Web interface lets you synchronize your IOS image and configuration files automatically, or on demand.

SD Card Synchronization

The SD card synchronization feature lets you synchronize the SD card with the onboard flash memory. You can synchronize either the configuration files or the IOS image. If the SD card is present, the switch starts from the SD card with its configuration. If the SD card is not present, the switch reads the start parameters from the specified IOS image stored on internal memory.

IMPORTANT You can overwrite your desired configuration if you synchronize in the wrong direction.

Alarms

You can connect up to two alarm inputs from external devices in your environment, such as a door or a temperature gauge, to the alarm input port on the switch front panel. Output alarm contacts can be configured by using the CLI. The default output is also triggered by an over- or under-temperature alarm or a port not forwarding condition. The output alarm relay can be configured as a normally energized or a normally de-energized circuit by using the CLI.

Cryptographic IOS Software (optional)

The Stratix 5700 cryptographic IOS (available as a separate catalog number for downloading) provides network security by encrypting administrator traffic during Telnet and SNMP sessions. The cryptographic IOS supports all features of the standard IOS, as well as these protocols:

- Secure Shell (SSH) Protocol v2

- SNMPv3
- HTTPS

Cable Diagnostics

The Cable Diagnostics feature lets you run a test on each switch port to determine the integrity of the cable connected to the RJ45 (copper) ports. This feature is not available for fiber ports.

The test determines the distance to the break from the switch for each cable with a plus or minus error value individually listed.

Advanced Software Features

More advanced software features are available, some of which are configured by the global macro or Smartports for typical automation applications described in this manual.

For information about how to configure features not available in the Device Manager Web interface or the Logix Designer application, see the following:

- Cisco IE2000 Switch Software Configuration Manual available at http://www.Cisco.com.
- Cisco IE2000 Switch Command-Line Interface Manual available at http://www.Cisco.com.

Notes:

Manage the Switch via the Device Manager Web Interface

Topic	Page
Access the Device Manager Web Interface	118
Dashboard Overview	119
Configure Smartports	125
Configure Port Settings	132
Configure Port Thresholds	134
Configure EtherChannels	135
Configure DHCP	137
Configure VLANs	141
Configure Power over Ethernet (PoE) Ports	142
Configure PTP Time Synchronization	145
Enable and Configure Routing	148
Configure STP	149
Configure REP	151
Configure NAT	153
Configure Port Security	162
Configure IGMP Snooping	164
Configure SNMP	165
Configure Alarm Settings	166
Configure Alarm Profiles	168
Monitor Trends	170
Monitor Port Statistics	171
Monitor NAT Statistics	172
Monitor REP Topology	173
Monitor CIP Status	174
Diagnose Cabling Problems	176
View System Log Messages	177
Use Express Setup to Change Switch Settings	178
Manage Users	180
Reallocate Switch Memory for Routing	181
Restart the Switch	182
Upgrade the Switch Firmware	183

Topic	Page
Use the SD Card to Synchronize the Configuration or IOS Files	184
Upload and Download Configuration Files	186
Upgrade License Files	186

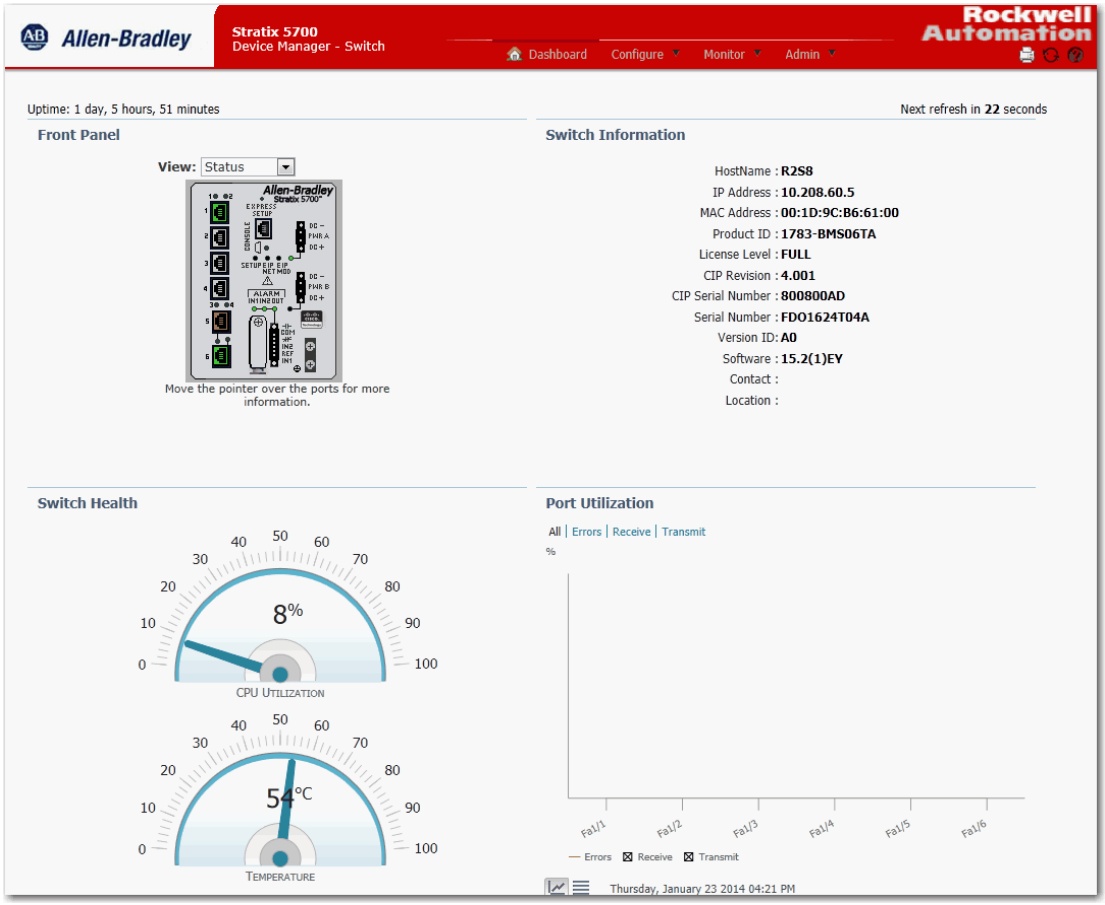
After you complete Express Setup, you can manage the switch by using the Device Manager Web interface supplied with the switch.

For simplicity, most of the illustrations in this chapter show a 6-port switch.

Access the Device Manager Web Interface

To access the Device Manager Web interface, follow these steps.

1. Launch a Web browser on your workstation.
2. Enter the switch IP address in the Web browser and click Enter.
3. Enter the user name and password.



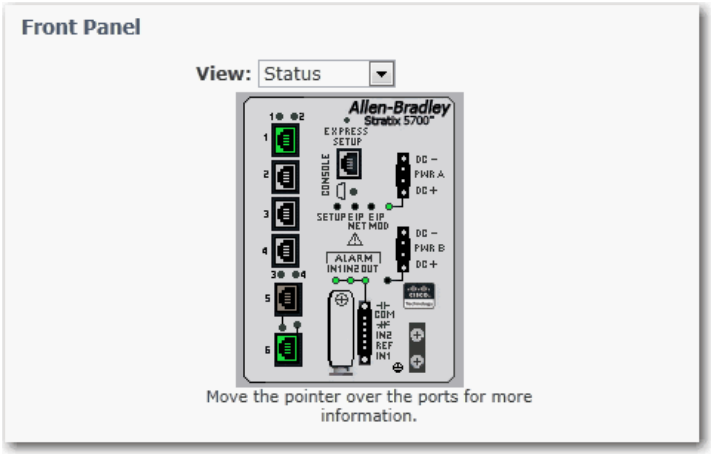
Dashboard Overview

You can use the dashboard to monitor switch status and performance.

The Dashboard window is similar to the Monitor > Trends window. The Dashboard window displays the instantaneous status while the Trends window displays the historical status. By using them together, you can gather the detailed conditions of the switch and its ports. For information about the Trends window, see page 170.

Front Panel and Status Indicators

The Front Panel view is a graphical display of the switch front panels.



The switch components on the front panel view are color-coded by status. The colors help you to quickly see if a fault or an error condition exists. The system-level status indicators and port-level status indicators shown on the front panel view match those on the physical switch.

Table 9 - Front Panel Status Indicators

Indicator	Status	Description
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Blinking green	The switch is not configured (for example, the switch does not have an IP address configured).
	Blinking red	The switch has detected a recoverable system fault.
	Solid red	The switch has detected a non-recoverable system fault.
	Blinking green and red	The switch is running its power-on self-test (POST).
DC_A DC_B	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present on the associated circuit.
	Solid red	Power is not present on the associated circuit, and the switch is configured for dual-input power.
Alarm Out	Off	Alarm Out not configured, or the switch is off.
	Solid green	Alarm Out is configured; no alarm is detected.
	Blinking red	The switch has detected a major alarm.

Table 9 - Front Panel Status Indicators (continued)

Indicator	Status	Description
Alarm In 1 Alarm In 2	Off	Alarm input not configured.
	Solid green	Alarm input configured; no alarm detected
	Blinking red	Major alarm detected.
	Solid red	Minor alarm detected.
Setup	Off	The switch is configured as a managed switch.
	Solid green	The switch is in initial setup.
	Blinking green	The switch is in initial setup, fault recovery, or initial setup is incomplete.
	Solid red	The switch failed to start initial setup or recovery because there is no available switch port to connect to the management station. Disconnect a device from a switch port, then press the Express Setup button on the switch.
Ports—Each combo port has two status indicators: one for the SFP module and one for the RJ45 connector. The appropriate status indicator is active for the active port.		
	Off	No link present on the port.
	Solid green	Port link; no activity.
	Flashing green and off	Link is active and healthy.
	Alternating green and amber	There is a fault or error on the link.
	Solid amber	The port is disabled.
EIP Net—The EIP Net status indicator shows the network status of the switch.		
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Blinking green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Blinking red	One or more connections to attached devices have timed out.
	Solid Red	The switch has detected that its IP address is already in use by another device in the network.
	Blinking green and red	The switch is running its power-on self-test (POST).
Status —In this mode, the port status indicators show the status of the ports. This is the default mode.		
	Off	No link.
	Solid green	No activity on link.
	Flashing green	Link activity.
	Solid brown	Port has been disabled.
	Yellow	An error has disabled the port.
	Flashing green and amber	Faulty link.
	Flashing amber	Smartports configuration mismatch on port.
	Solid amber	Port is faulty, disabled due to an error, or is in an STP-blocked state.
Smartports—In this mode, each port image shows the applied port role. For information about Smartports, see Optimize Ports through Smartports Port Roles on page 83.		

You can change the port status indicator behavior by choosing a Port mode from the View list on the front panel view.

Move the pointer over a port to display specific information about the port and its status.

TIP If you move the pointer over a port that is blinking green and amber, the status is one of the following:

- Link is faulty
- Link has collisions

In either state, the port is receiving and sending traffic.

Note the following:

- The speed and Duplex mode for a port appear only when a device is connected to the port.
- For dual-purpose ports, the Type field displays 10/100/1000BaseTX for the copper uplink port whether or not the port is active. The Type field also displays either the type of SFP module installed or Empty if a module is not installed.
- The Smartport type and VLAN type and name are displayed when Smartport Port mode is selected.
- The Uptime field shows how long the switch has been operating since it was last powered on or was restarted. Status is automatically refreshed every 60 seconds or when you click Refresh. The refresh counter shows the number of seconds that remain before the next refresh cycle starts.

Switch Information

The Switch Information area on the Dashboard displays information about the switch, as described in the following table.

Field	Description
Host Name	A descriptive name for this switch. The default name is Switch. You can set this parameter on the Admin > Express Setup window.
IP Address	The IP address of this switch. You can configure this setting on the Admin > Express Setup window.
MAC Address	The MAC address of this switch. This information cannot be changed.
Product ID	The model of this switch. This information cannot be changed.
License Level	The type of license that is installed. This information cannot be changed.
CIP Revision	The version of Common Industrial Protocol (CIP) that is supported on this switch. This information cannot be changed.
CIP Serial Number	The CIP serial number. This information cannot be changed.
Serial Number	The serial number of this switch. This information cannot be changed.
Version ID	The hardware version. This information cannot be changed.
Software	The version of IOS that this switch is running. This information is updated when you upgrade the switch firmware.
Contact	The person who is the administrative contact for this switch. You can set this parameter on the Configure > SNMP window.
Location	The physical location of this switch. You can set this parameter on the Configure > SNMP window.

Switch Health

You can use the health gauges to monitor the switch.

CPU Utilization

The CPU Utilization gauge shows the percentage of CPU processing power that is in use on the switch. Data is collected at each 60-second system refresh. The gauge changes as the switch experiences the network activity from devices sending data through the network. As network activity increases, so does contention between devices to send data through the network.

As you monitor utilization on the switch, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, perhaps a problem exists. As you monitor the switch, note if the bandwidth utilization is consistently high. This can mean there is congestion in the network. If the switch reaches its maximum bandwidth (above 90% utilization) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the switch is configured to help recover lost packets, such as by signaling to other devices to resend data. However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, that can also increase bandwidth utilization on the switch.

Temperature

The Temperature gauge shows the internal temperature of the switch. For information about the switch temperature range and the operating environment guidelines, see the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

Port Utilization

You can choose which types of network traffic to display and in what format:

- Types of traffic—By default, all traffic is displayed for all interfaces. Click the links above the display area to display all traffic, errors, received traffic, or transmitted traffic.
- Formats—Click the buttons below the display area to view the data in Chart Mode or Grid Mode.
- Chart details—When displaying a chart, position your mouse pointer over a bar or a point on the chart to view the data.

As you monitor the usage on the ports, note whether the percentage is what you expect during that given time of network activity. If usage is high when you expect it to be low, a problem can exist. Bandwidth allocation can also be based on whether the connection is operating in half-duplex or full-duplex mode.

These are some of the reasons for errors received on or sent from the switch ports:

- Bad cable connection
- Defective ports
- Software problems
- Driver problems

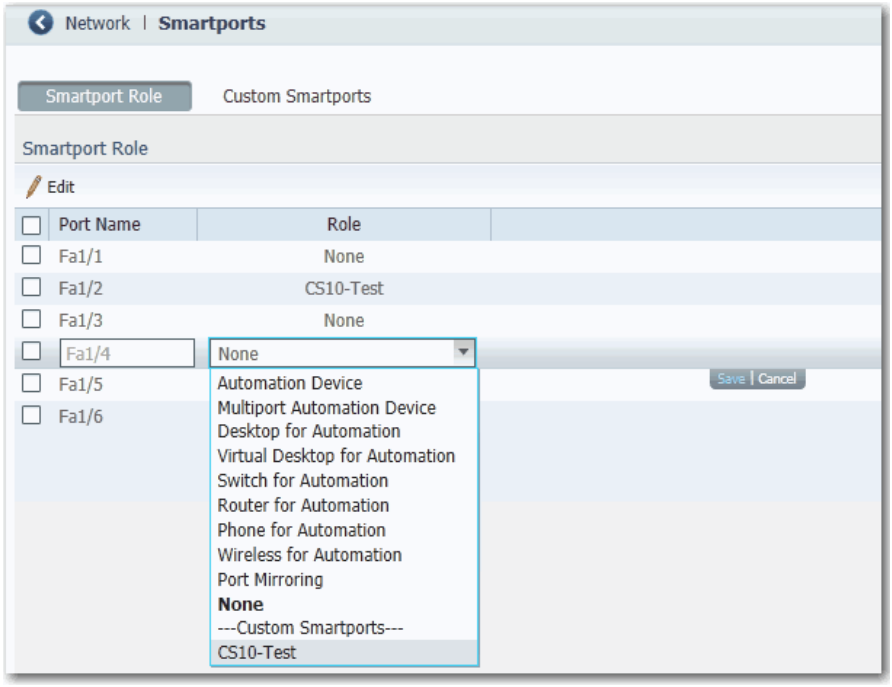
Data is collected at each 60-second system refresh.

Refer to Monitor Trends on page 170 for a graph to view per-port patterns over incremental instances in time (by 60 seconds, 1 hour, 1 day, or 1 week).

Refer to Monitor Port Statistics on page 171 for details on the specific port errors detected on each port.

Configure Smartports

To assign Smartport roles to switch ports, from the Configure menu, choose Smartports.



Follow these guidelines when using Smartport roles:

- Before using Smartport roles, decide which switch port is connected to which device type.
- Before attaching a device to the port or reconnecting devices that have been moved, verify which Smartport role is applied to a port.

  IMPORTANT We recommend that you do not change port settings after enabling a Smartport role on a port. Any port setting changes can alter the effectiveness of the Smartport role.

- When the user attempts to apply a port role to a routed port in the Smartports window, this error message appears:

  A port role cannot be configured on a routed port.

To apply a Smartport role, follow this procedure.

1. From the Configure menu, choose Smartports.
2. Select a port.
3. Choose a Smartport role from the pull-down menu in the Role column.
4. Click Save.

Customize Port Role Attributes

Each switch port is a member of a VLAN. Devices attached to switch ports that belong to the same VLAN share the same data broadcasts and system resources.

Depending on your network requirements, it can be sufficient to assign all ports to the default VLAN, which is named default. One VLAN can be sufficient for a small network.

Before changing virtual local-area network (VLAN) memberships, understand what a VLAN is, its purpose, and how to create a VLAN. See page 90 for more information about VLANs.

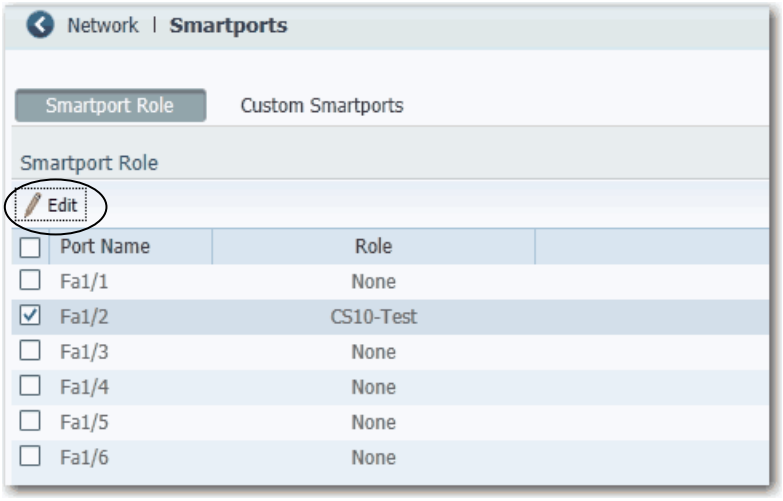
Assign a Port to a VLAN (VLAN memberships)

Each switch port is a member of a VLAN. Devices attached to switch ports that belong to the same VLAN share the same data broadcasts and system resources. Communication between VLANs requires a Layer 3 device (such as a router or a Layer 3 switch).

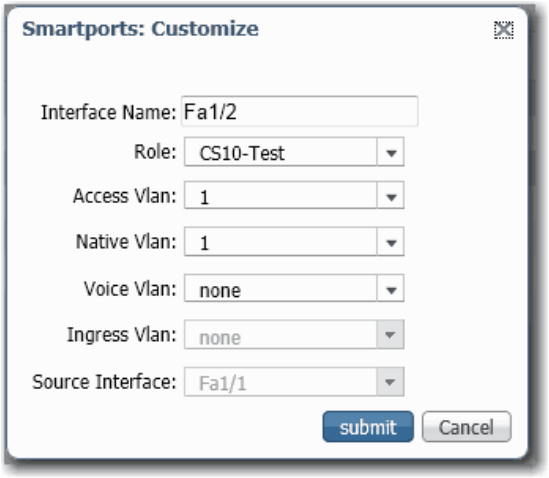
Depending on your network requirements, it can be sufficient to assign all ports to the default VLAN, which is named default. If additional VLANs have been created, you must decide which ports are best suited to which VLANs.

To change a VLAN assignment, follow these steps.

1. From the Configure menu, choose Smartports.
2. Check the checkbox next to the port for which to change the VLAN.
3. Click Edit.



4. Modify the VLAN assignments as needed:
   - For ports applied with the Automation Device with QoS, Switch For Automation, Router For Automation, or Wireless For Automation port role, choose a VLAN from the Native VLAN list.
   - For ports applied with the Automation Device, Desktop For Automation, Phone For Automation, or None port role, choose a VLAN from the Access VLAN list.
   - For ports applied with the Phone For Automation port role, choose a VLAN from the Voice VLAN list.
   - For ports applied with the Port Mirroring port role, choose a VLAN from the Ingress VLAN list and choose the port to be monitored from the Source Interface list.



5. Click Submit.

Manage Custom Smartport Macros

To create a custom Smartports macro, follow these steps.

1. Click the Custom Smartports tab.
2. Click Add.
3. Enter the name for the macro.

   Macro names are case sensitive. The string can be up to 31 alphanumeric characters. The string cannot contain a ?, a space, or a tab.
4. Choose a macro icon (CS1 to CS10).

5. Enter a macro definition.

   The definition can contain up to 3000 characters. Enter the macro commands with one command per line. Use the # character at the beginning of a line to enter comment text within the macro.

   Available parameters for the macro are $native_vlan, $access_vlan, and $voice_vlan.

6. Enter an antimacro definition.

   The antimacro definition is the portion of the applied macro that removes the macro when you change it to another macro or when you remove it with the None Smartport role. Before the macro definition can be applied to the port, the antimacro must first be defined with the proper commands to set the port back to its original state.

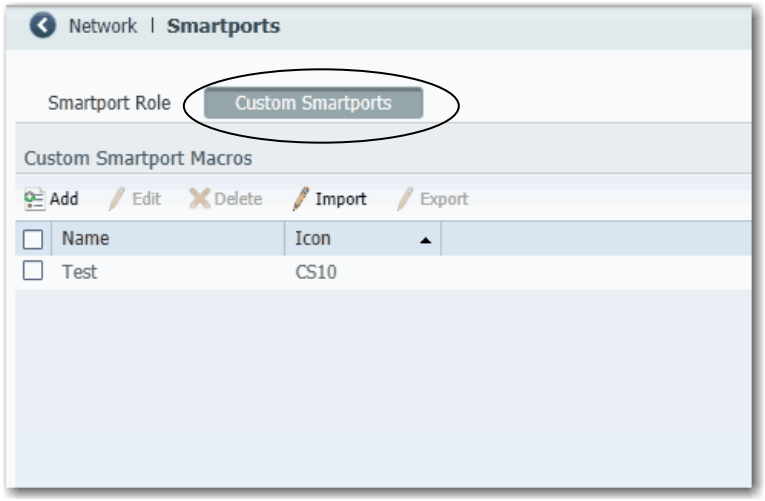
   The definition can contain up to 3000 characters. Enter the antimacro commands with one command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

7. Click Submit.
8. To discard any unsaved changes, click Cancel.

Modify the Definition of a Custom Smartports Macro

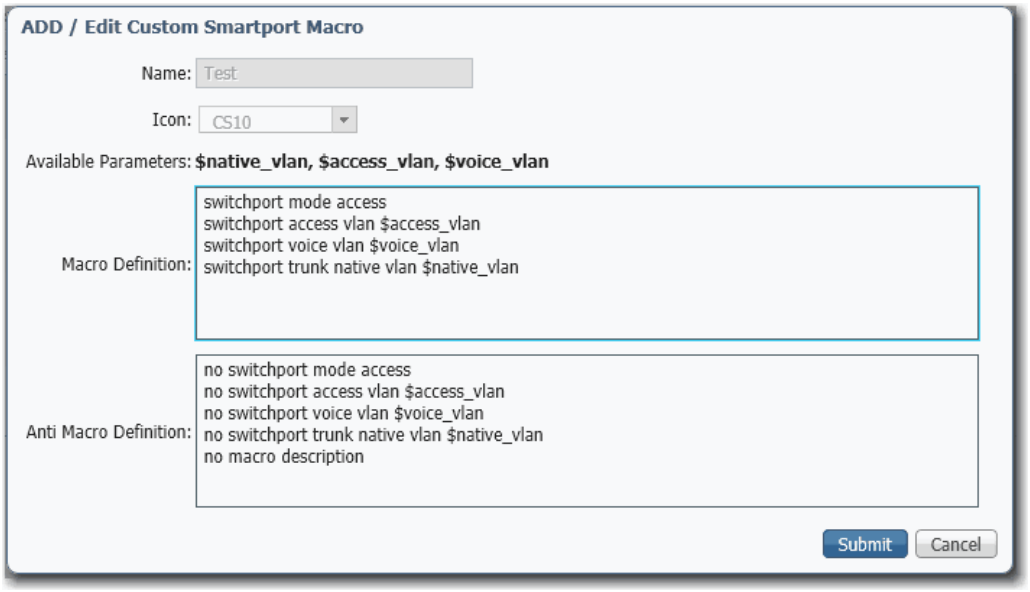
You cannot modify a custom Smartports macro that is currently in use.

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.



3. Check the checkbox next to the macro to modify.

4. Click Edit.

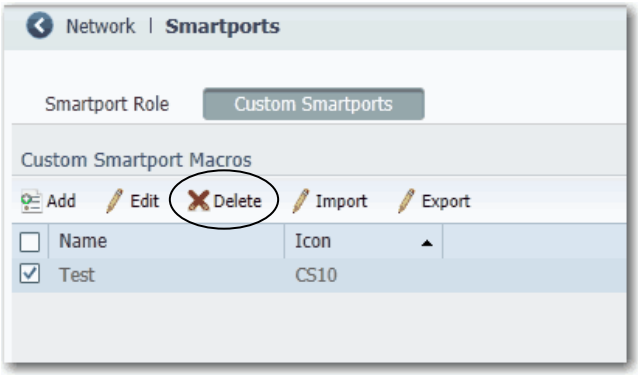


5. Change the definitions as needed.
6. Click Submit.

Delete a Custom Smartports Macro

You cannot delete a custom Smartports macro that is currently in use.

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Check the checkbox next to the macro to delete.

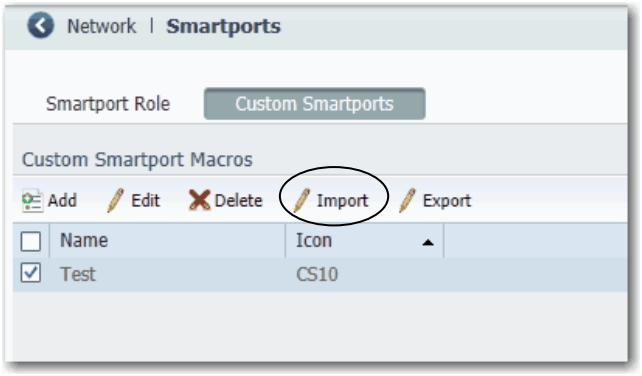


4. Click Delete.

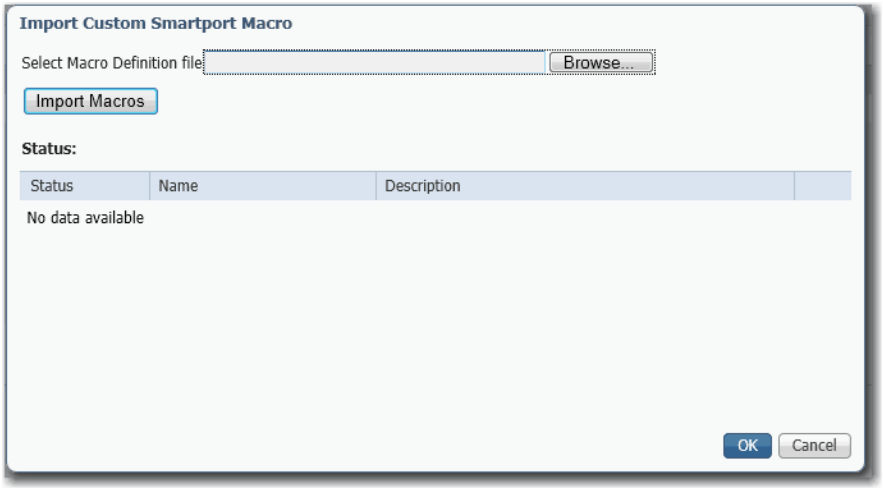
Import a Custom Smartports Macro

You must use Firefox 3.6 or higher to import a custom Smartports macro.

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Click Import.



4. Click Browse.



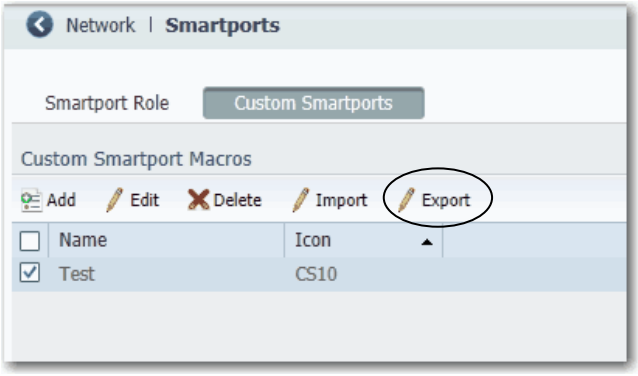
5. Select the macro file on your computer or network drive.

   The file must be an appropriately formatted .xml file.
6. Click Import Macros.
7. Click OK.

Export a Custom Smartports Macro

You must use Firefox 3.6 or higher to export a custom Smartports macro.

1. From the Configure menu, choose Smartports.
2. Click the Custom Smartports tab.
3. Check the checkbox next to the macro to export.
4. Click Export.



5. Save the resulting file.

Configure Port Settings

The basic port settings determine how data is received and sent between the switch and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port must be compatible with the port settings of the connected device.

To change basic port settings, from the Configure menu, choose Port Settings.

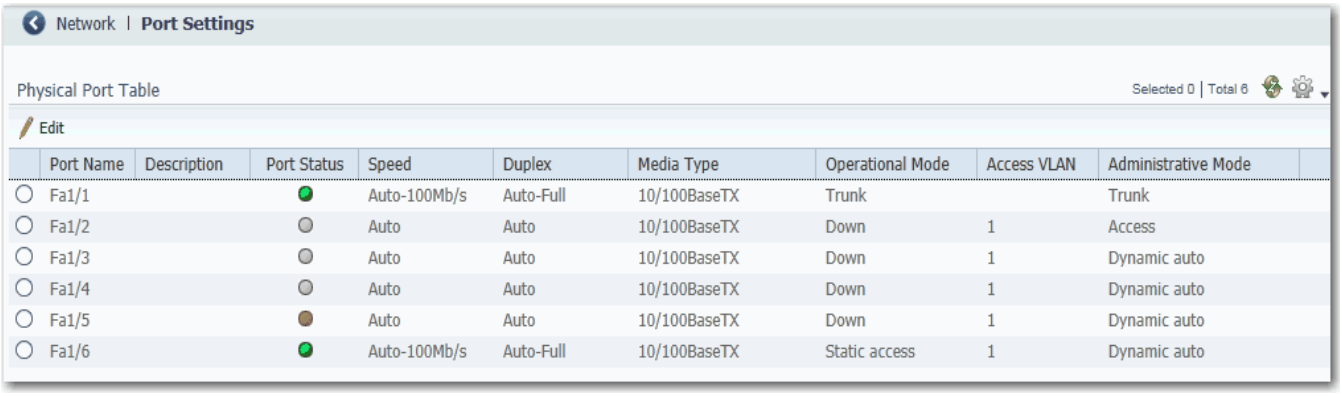


Table 10 lists the basic settings for the switch ports. To change these settings, click the radio button next to the port name and click Edit to display the Edit Physical Port window.

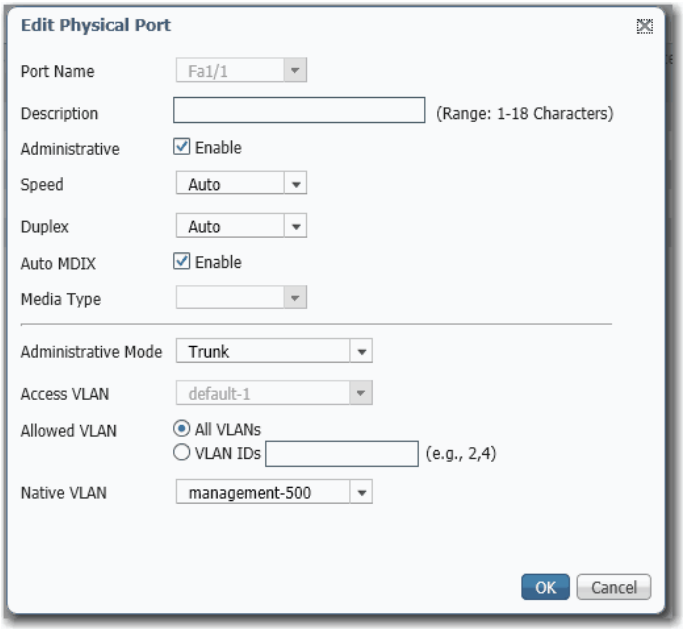


Table 10 - Port Settings

Field	Description
Port Name	The number of the switch port, including port type, such as Fa for Fast Ethernet and Gi for Gigabit Ethernet, and the specific port number: • Gi/1 is the gigabit port 1 of the switch. • Fa1/1 is Fast Ethernet port 1 on the switch.
Description	The description of the switch port. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Port Status	The state of the switch port. The default is Enabled. You can change this setting on the Edit Physical Port window by checking or clearing the Administrative checkbox. We recommend disabling the port if the port is not in use and is not attached to a device. An example of when to change this setting is during troubleshooting. You can troubleshoot a suspected unauthorized connection by administratively disabling the port.
Speed	The operating speed of the switch port. You can choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default is Auto. We recommend that you use the default so that the speed setting on the switch port automatically matches the setting on the connected device. Change the switch port speed if the connected device requires a specific speed. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to see if the switch port and connected device have a speed mismatch.
Duplex	The Duplex mode of the switch port: • Auto (autonegotiation) if the connected device can negotiate with the switch. • Full (Full-duplex mode) if both devices can send data at the same time. • Half (Half duplex mode) if one or both devices cannot send data at the same time. The default is Auto. On Gigabit Ethernet ports, you cannot set the port to Half-duplex mode if the port speed is set to Auto. We recommend that you use the default so that the duplex setting on the switch port automatically matches the setting on the connected device. Change the Duplex mode on the switch port if the connected device requires a specific mode. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to verify if the switch port and connected device have a duplex mismatch.
Auto-MDIX	Whether the automatic medium-dependent interface crossover (auto-MDIX) feature can automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately. The default is Enable. This setting is not available on the SFP module ports.
Media Type	The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port. By default, the switch detects whether the RJ45 port or SFP module port of a dual-purpose port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected, the SFP module port has priority. You cannot change the priority setting. Choose from the following media types: • SFP—The SFP module port is active. If you choose this option, the speed and duplex displays the current settings and auto-MDIX displays N/A. • RJ45—The RJ45 port is active. If you choose this option, you can set the port speed, duplex, and auto-mdix values. • Auto (autonegotiation)—Either port can be active. If you choose this option, the speed and duplex is set to auto and auto-MDIX displays N/A. The default is Auto.

Table 10 - Port Settings (continued)

Field	Description
Operational Mode	The operational state of the port. Displays the administrative mode or Down (if disabled).
Access VLAN	The VLAN that an interface belongs to and carries traffic for, when the link is configured as or is acting as a nontrunking interface.
Administrative Mode	Displays one of the following administrative modes: • Access—The interface is in permanent nontrunking mode and negotiates to convert the neighboring link into a nontrunk link even if the neighboring interface is a trunk interface. If you choose this option, also choose an Access VLAN. An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). • Trunk—The interface is in permanent trunking mode and negotiates to convert the neighboring link into a trunk link even if the neighboring interface is not a trunk interface. If you choose this option, also choose whether to allow All VLANs or specified VLAN IDs • Dynamic Auto—The interface converts the link to a trunk link if the neighboring interface is set to trunk or desirable mode. This mode is the default setting. If you choose this option, specify an Access VLAN to use when the link is in access mode. Also specify whether to allow All VLANs or specified VLAN IDs when the link is in trunk mode. • Dynamic Desirable—The interface converts the link to a trunk link if the neighboring interface is set to Trunk, Dynamic Desirable, or Auto mode. If you choose this option, specify an Access VLAN to use when the link is in access mode. Also choose whether to allow All VLANs or specified VLAN IDs when the link is in Trunk mode.

Configure Port Thresholds

Configure port thresholds to prevent traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces.

To configure port thresholds, from the Configure menu, choose Port Thresholds.

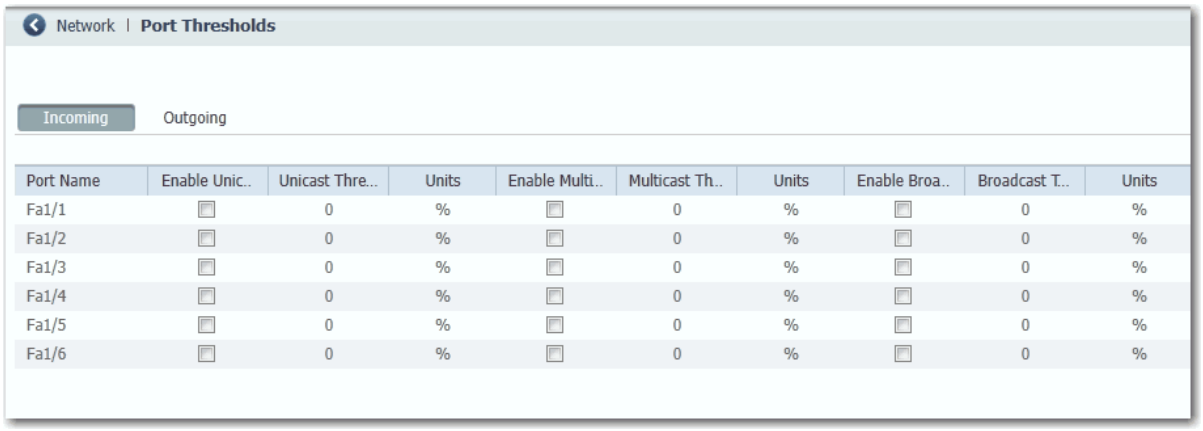


Table 11 - Port Threshold Fields

Field	Description
Incoming	
Unicast	For each port, do the following: 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Choose one of these units: – PPS (0…10 billion) – BPS (0…10 billion) – % (0…100)
Multicast	
Broadcast	
Outgoing	
All Traffic	For each port, do the following: 1. Check or clear the Enable checkbox. 2. Type the threshold value. 3. Click Save.

Configure EtherChannels

An EtherChannel, or port group, is a group of two or more switch ports bundled into a single logical link to create a higher bandwidth link between two switches.

For example, four 10/100 switch ports can be assigned to an EtherChannel to provide full-duplex bandwidth of up to 800 Mb/s. If one of the ports in the EtherChannel becomes unavailable, traffic is carried over the remaining ports within the EtherChannel.

All ports in an EtherChannel must have the same characteristics:

- All are applied with the Smartports IE Switch port role and belong to the same VLAN.
- All are either 10/100 ports, or all are 10/100/1000 ports. You cannot group a mix of 10/100 and 10/100/1000 ports in an EtherChannel.
- All are enabled. A disabled port in an EtherChannel is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.

IMPORTANT Do not enable Layer 3 addresses on the physical EtherChannel interfaces.

To create, modify, and delete EtherChannels, from the Configure menu, choose EtherChannels.

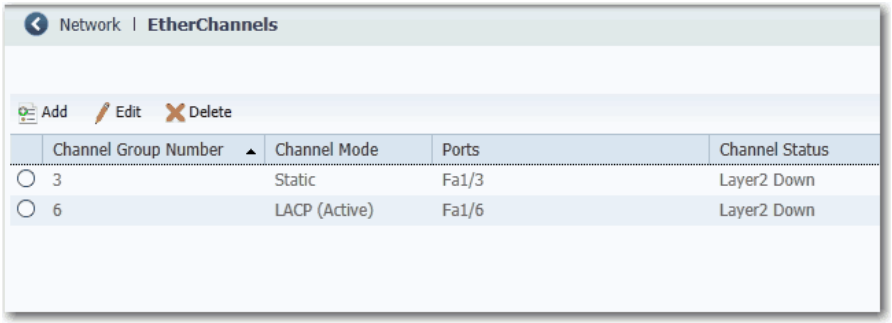


Table 12 - EtherChannel Fields

Field	Description
Channel Group Number	A number from 1 to 6 that identifies this EtherChannel. You can configure as many as six EtherChannels.
Channel Mode	Determines how ports become active. With all options except On, negotiations occur to determine which ports become active. Incompatible ports are put into an independent state and continue to carry data traffic, but do not participate in the EtherChannel. **IMPORTANT:** Ensure that all of the ports in an EtherChannel are configured with the same speed and duplex mode. These are the available modes: • Static—All ports join the EtherChannel, without negotiations. This mode can be useful if the remote device does not support the protocols required by the other modes (see below). The switches at both ends of the link must be configured in On mode. • PAgP—This mode enables Port Aggregation Protocol (PAgP), a Cisco-proprietary protocol. The port responds to requests to create EtherChannels but does not initiate such negotiations. This "silent" mode is recommended when a port is connected to a device, such as a file server or a packet analzyer, that is unlikely to send PAgP packets. A port in the Auto mode can form an EtherChannel with another port in the Desirable mode. • PAgP (non-silent)—This mode is the same as Auto mode but is recommended when the port is connected to a device that is expected to be active in initiating EtherChannels. A port in the Auto mode can form an EtherChannel with another port in the Desirable mode. • PAgP Desirable—This mode enables Port Aggregation Protocol (PAgP), a Cisco-proprietary protocol. The port initiates negotiations to form EtherChannels by sending PAgP packets to other ports. This "silent" mode is recommended when a port is connected to a device, such as a file server or a packet analzyer, that is unlikely to send PAgP packets. A port in the Desirable mode can form an EtherChannel with another port that is in the Desirable or Auto mode. • PAgP Desirable (non-silent)—This mode is the same as Desirable mode but is recommended when the port is connected to a device that is expected to be active in initiating EtherChannels. • LACP (Active)—This mode enables Link Aggregation Control Protocol (LACP) unconditionally. The port sends LACP packets to other ports to initiate negotiations to create EtherChannels. A port in Active mode can form an EtherChannel with another port that is in Active or Passive mode. The ports must be configured for full duplex. • LACP (Passive)—This mode enables Link Aggregation Control Protocol only if an LACP device is detected at the other end of the link. The port responds to requests to create EtherChannels but does not initiate such negotiations. The ports must be configured for full duplex.
Ports	The ports that can participate in this EtherChannel.
Channel Status	The status of the group.

Configure DHCP

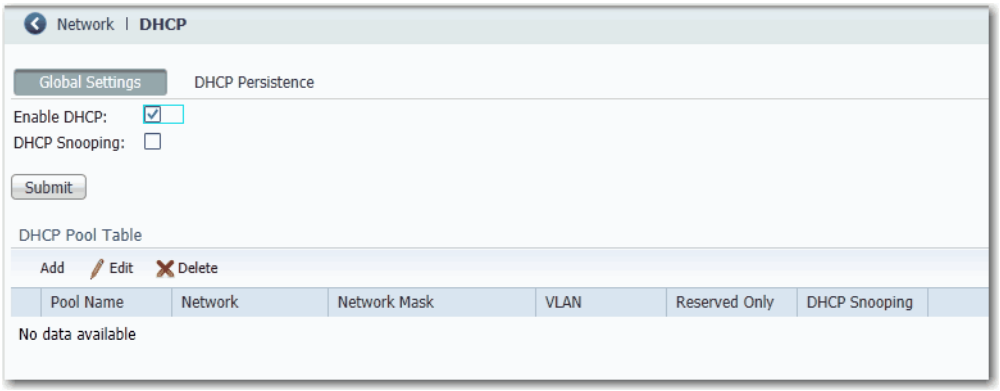
To use DHCP persistence, you must first enable DHCP and set up the IP address pool. Then you must assign a specific IP addresses to each port.

Set up the DHCP Server

To enable the DHCP Server mode on the switch, do the following.

1. From the Configure menu, choose DHCP.
2. Check the Enable DHCP checkbox.
3. To enable DHCP snooping, check the DHCP Snooping checkbox.

   DHCP snooping restricts broadcast of DHCP requests beyond the connected switch.This means that devices receive address assignments from only the connected switch. This option is available only on VLAN interfaces. To enable DHCP Snooping on a specific VLAN, check the DHCP Snooping checkbox for the specific VLAN in the DHCP pool table.



4. To reserve an address pool to only the devices that are specified in the DHCP persistence table, check the Reserved Only checkbox in the DHCP pool table.

   DHCP requests from ports not in the persistence table or from another device (switch) are ignored. By default, this option is disabled and the Reserved Only checkbox is cleared.

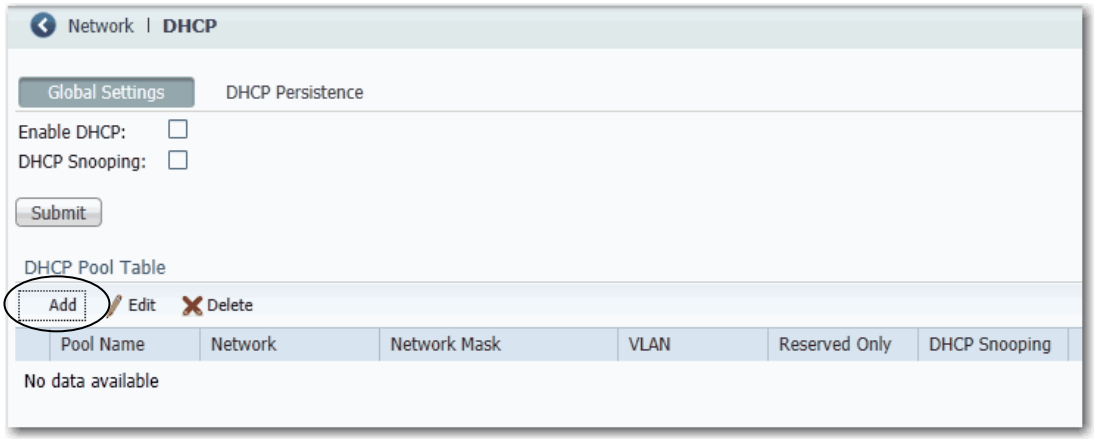
5. Click Submit.

Configure a DHCP IP Address Pool

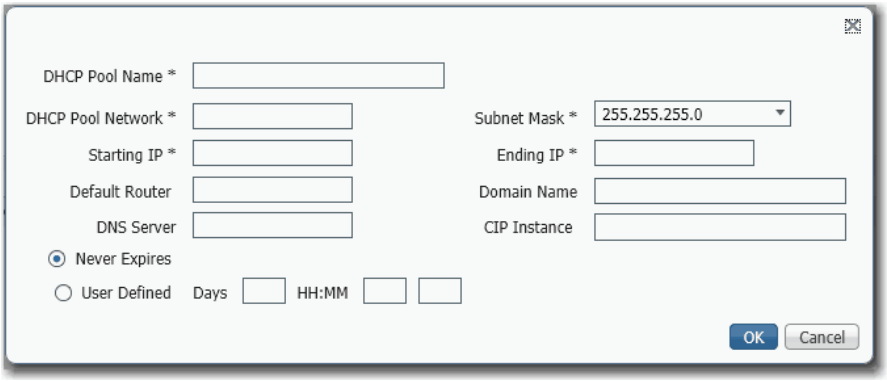
Once DHCP is enabled, you can create the DHCP address pool.

To configure a DHCP IP address pool, follow these steps:

1. From the Configure menu, choose DHCP.
2. Click Add.



3. Complete the fields as described below and click OK.



Field	Description
DHCP Pool Name	The name of the DHCP IP address pool configured on the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab. This field is required. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices.
DHCP Pool Network	The subnetwork IP address of the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. This field is required.
Subnet Mask	The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is required.
Starting IP	The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Be sure that none of the IP addresses that you assign are being used by another device in your network. This field is required.

Field	Description
Ending IP	The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that none of the IP address you assign are being used by other devices in your network. This field is required.
Default Router	The default router IP address for the DHCP client that uses this server. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0… 255.
Domain Name	The domain name for the DHCP client. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
DNS Server	The IP addresses of the Domain Name System (DNS) IP servers available to a DHCP client. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255.
CIP Instance	A number from 1…15 to identify the address pool.
[Lease Length]	The duration of the lease for an IP address that is assigned to a DHCP client. Click one of the following: • Never Expires • User Defined If you click User Defined, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.

Reserve IP Addresses through DHCP Persistence

You can reserve and preassign an IP address from the IP address pool to a specific switch port, so that a device connected to that switch port always receives the same IP address regardless of its MAC address.

DHCP persistence is useful in networks that are set up in advance, where dependencies on the exact IP addresses of some devices exist. Use DHCP persistence when the attached device has a specific role to play and when other devices know its IP address. If the device is replaced, the replacement device is assigned the same IP address, and the other devices in the network require no reconfiguration.

When the DHCP persistence feature is enabled, the switch acts as a DHCP server for other devices on the same subnet, including devices connected to other switches. If the switch receives a DHCP request, it responds with any unassigned IP addresses in its pool. To prevent this from happening, check the Reserve Only box on the DHCP window. This prevents the switch from responding when it receives a request.

When DHCP persistence is enabled on a port and a DHCP request is made from a connected device on that port, the switch assigns the IP address for that port in the DHCP window. It also broadcasts the DHCP request to the remainder of the network. If another DHCP server with available addresses is on the network and receives this request, it can try and respond. This can override the initial IP address assigned by the switch depending on how the end device behaves (takes first IP address response or the last). To prevent the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. Doing this blocks the broadcast of this DHCP request, so that no other server, including another Stratix switch with DHCP persistence enabled, responds.

If you are using DHCP persistence, we recommend that you initially assign static IP addresses to end devices. If an end device fails and is replaced, the DHCP persistence feature assigns an IP address from the DHCP persistence table. The device functions properly with this IP address, but we recommend that you reassign a static IP address to the replaced devices.

The following figure and table illustrate DHCP persistence behavior.

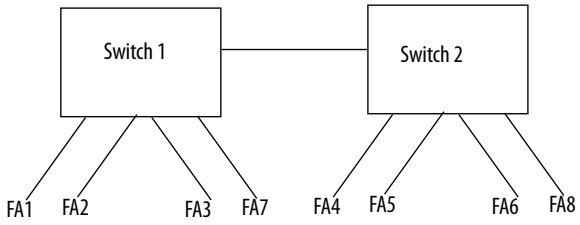


Table 13 - DHCP Persistence Behavior

If	Then
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is not selected and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 responds if there is an unassigned address in its pool. This can override the assignment made by switch 1.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in both switches and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. Note that if the device is connected to FA7 of switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in switch 1 and DHCP snooping is off, but not switch 2 when DHCP snooping is off	A new device is connected to FA1 receives an IP address from the persistence table. A broadcast request is also sent across the network. Switch 2 does not respond to the request. In addition, a device connected to FA4 receives an IP address from the switch 2 persistence table. A broadcast request is sent out, and switch 1 responds with an unused IP address from its pool.This can override the assigned port.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is checked	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 does not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it does not receive an IP address from the switch pool because it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved Only is not checked	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 does not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it receives an unassigned IP address from the Switch 1 pool.

To assign, modify, or delete a switch port IP address, click the DHCP Persistence tab.

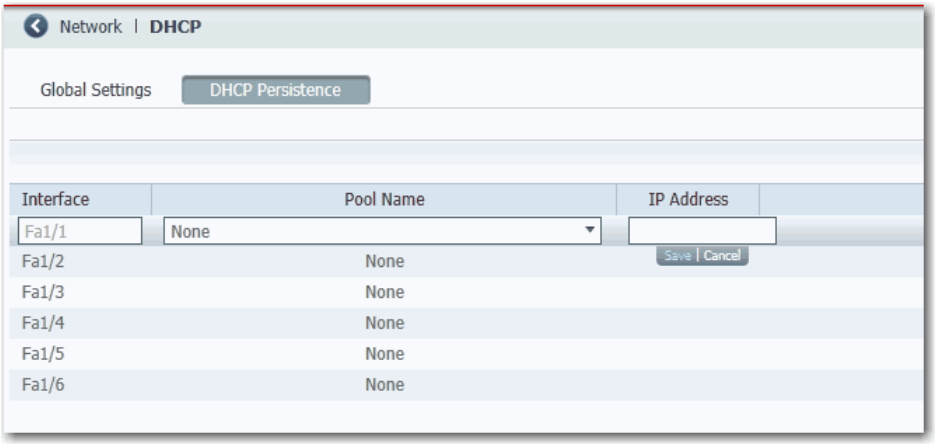
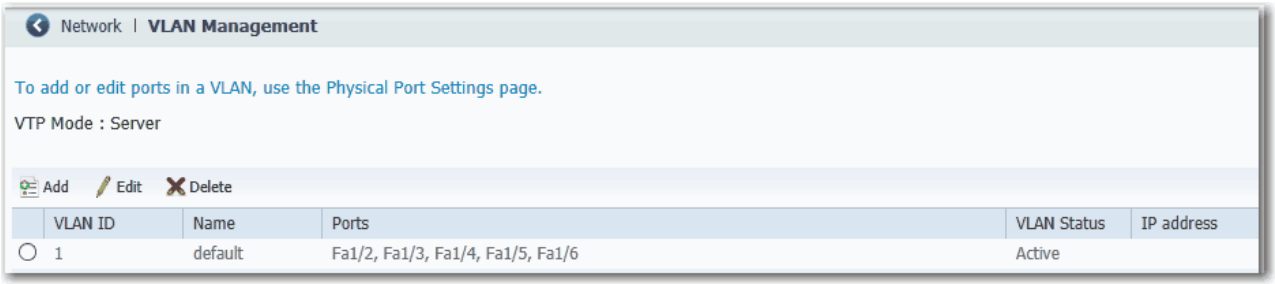


Table 14 - DHCP Persistence Fields

Field	Description
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. For example, Fa1/1 is Fast Ethernet port 1 on the switch.
Pool Name	The name of the DHCP IP address pool configured on the switch.
IP Address	The IP address assigned to the switch port. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool specified in the DHCP Pool Name field.

Configure VLANs

To create, modify, and delete VLANs, from the Configure menu, choose VLAN Management.



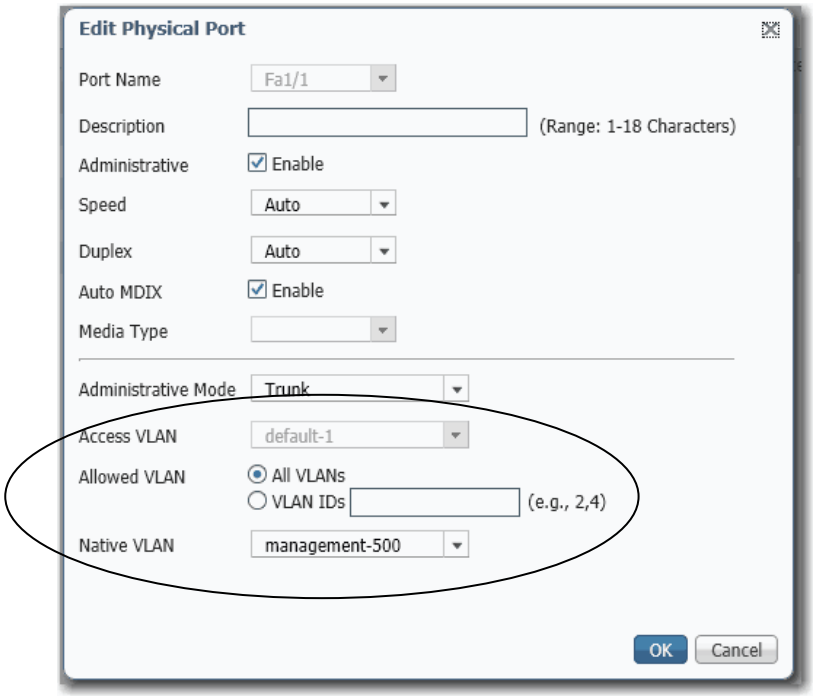
The default VLAN ID is 1 and the name for the management VLAN is default. The default VLAN alone can be sufficient based on the size and requirements of your network. We recommend that you determine your VLAN needs before creating VLANs.

To create a VLAN, you must give the VLAN a name and a unique ID number. You can modify the name of a VLAN but not its number. You cannot modify or delete the default VLAN.

After creating VLANs, you can then assign ports to VLANs. Before assigning ports to VLANs, make sure that each port has the appropriate port role.

Assign Ports to VLANs

To assign ports to VLANs, use the Edit Physical Ports window, as described on page 132.



Configure Power over Ethernet (PoE) Ports

PoE and PoE+ features are supported on switches with PoE ports when a correct power supply is connected to the switch. For power supply requirements, see page 44.

You can do the following from the PoE window:

- Limit the total power supported.
- Configure mode and power settings for individual ports.

For most applications, the default configuration (Auto mode) is sufficient and no further configuration is required. However, you can customize the settings to meet your needs. For example, to give a PoE port higher power priority, set the mode to Static and allocate the power to be used. As another example, to disallow

high-power devices on a port, set the mode to Auto and specify a maximum power limit.

IMPORTANT When you make PoE configuration changes to a port, the port drops power. Whether the port powers up again depends on the new configuration, the state of the other PoE ports, and the state of the power budget.

For example, if port 1 is in Auto mode and the On state, and you configure it for Static mode, the switch removes power from port 1, detects the powered device, and repowers the port.

If port 1 is in Auto mode and the On state and you configure it with a maximum wattage of 10 W, the switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

To configure PoE ports, from the Configure menu, choose Power Management.

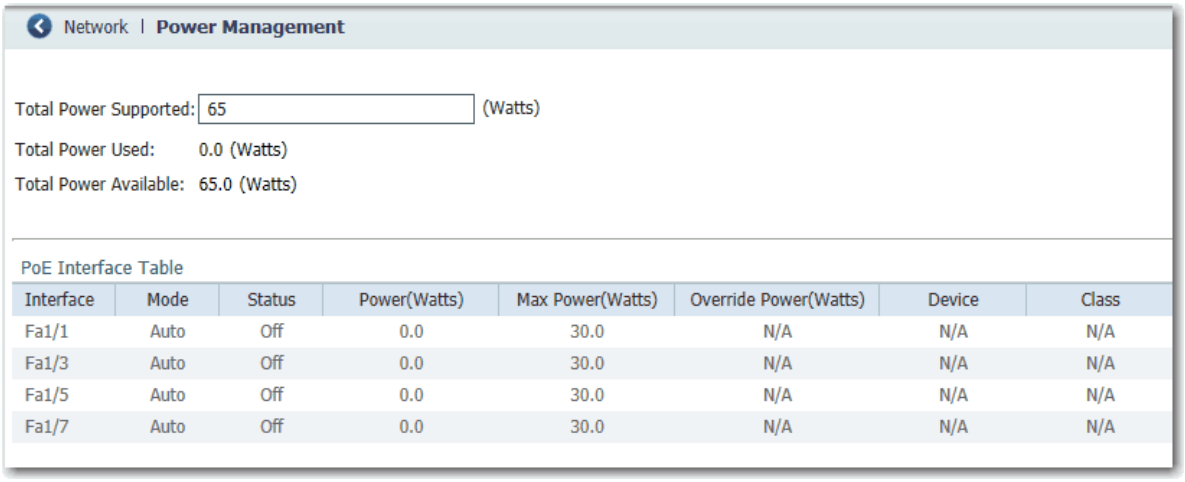

Network | Power Management
Total Power Supported: 65 (Watts)
Total Power Used: 0.0 (Watts)
Total Power Available: 65.0 (Watts)
PoE Interface Table
Interface Mode Status Power(Watts) Max Power(Watts) Override Power(Watts) Device Class
Fa1/1 Auto Off 0.0 30.0 N/A N/A N/A
Fa1/3 Auto Off 0.0 30.0 N/A N/A N/A
Fa1/5 Auto Off 0.0 30.0 N/A N/A N/A
Fa1/7 Auto Off 0.0 30.0 N/A N/A N/A

Table 15 - Power Management Fields

Field	Description
Total Power Supported	To limit the total PoE power budget, type an appropriate value based on the power source: • A 48V power source supports a maximum of 65 W. • A 54V power source supports a maximum of 130 W. When you save this setting, it changes the total PoE power budget and resets the powered devices to meet the new budget. **IMPORTANT:** A mismatch between the total power supported and the power supply can cause damage to the switch. Take care not to oversubscribe the power supply: • If you intend to connect the switch to a power supply that allows more wattage than configured, first change the power supply and then specify the total power supported. • If you intend to connect the switch to a power supply that allows less wattage than configured, first change the total power supported to an appropriate value and then change the power supply.
Total Power Used	Displays the amount of power the module is currently using.
Total Power Available	Displays the amount of unused power available to the module.
Interface	Displays the port number.

Table 15 - Power Management Fields

Field	Description
Mode	Displays the Power Management mode of the port: • Auto—Enables the detection of powered devices and automatically allocates power to the PoE port if a device is connected. This setting is selected by default. To limit the power used by this port, adjust the Max Power setting. • Static—Reserves power for this port even when no device is connected to make sure that power is provided upon device detection. You can also choose Static mode to prioritize a port. The switch allocates power to Static mode ports before it allocates power to Auto mode ports. • Off—PoE is disabled. For more information, see Power Management Modes on page 87.
Status	Displays whether PoE is enabled (on) or disabled (off) on the port.
Power (Watts)	Displays the amount of power allocated to the port.
Max Power (Watts)	Displays the maximum amount of power available to the port: PoE ports: 4…15.4 W PoE+ ports: 4…30 W
Override Power (Watts)	Indicates the power override configured for the port. This configuration overrides both the IEEE classification shown in the Class column and power negotiation. If no override is configured, the field displays N/A. You can configure a power override only by using the command line interface (CLI). For more information, refer to the Cisco IE-3000 Software Configuration Guide. **EXAMPLE** An administrator can choose to configure an override when the power requirement of a connected device is known and is less than the maximum value for the class. For instance, if a device requires only 5 W but is in Class 0, which allows a maximum of 15.4 W, configuring an override allows more power to other devices.
Device	Displays the device connected to the port. If no device is connected to the port, the field displays N/A.
Class	Displays the power classification of the powered device (PD). For power classification descriptions, see Table 5 on page 86.

Configure PTP Time Synchronization

The IEEE 1588 standard defines a protocol, called Precision Time Protocol (PTP), which enables precise synchronization of clocks in measurement and control systems. The clocks communicate with each other over the EtherNet/IP communication network. The PTP protocol enables heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the Grandmaster clock.

By default, PTP is disabled on all the Fast Ethernet and Gigabit Ethernet ports on the switch.

The switch supports these Synchronization Clock modes:

- **End-to-End Transparent mode**—The switch transparently synchronizes all slave clocks with the master clock connected to the switch.

  The switch corrects the delay incurred by every packet passing through the switch (referred to as residence time). This mode causes less jitter and error accumulation than Boundary mode.

  In End-to-End Transparent mode, all switch ports are enabled by default.

- **Boundary mode**—The switch becomes the parent clock to which the other devices connected to the switch synchronize their internal clocks.

  The switch and connected devices constantly exchange timing messages to correct time skew caused by clock offsets and network delays.

  This mode can eliminate the effects of latency fluctuations. Because jitter and errors can accumulate in cascaded topologies, use this mode for networks with only less than four layers of cascaded devices.

  In Boundary mode, one or more switch ports can be PTP-enabled.

- **Forward mode (default)**—Traffic is forwarded through the switch (while being prioritized by QoS) but is not acted on by the switch.

IMPORTANT When changing the PTP timing message settings, remember that the system does not operate properly unless all devices in the system have the same values.

To configure PTP, from the Configure menu, choose PTP.

Once you choose a mode, you can edit the settings for each port. The parameters depend on the selected mode. You can configure per-port PTP when the switch is in Boundary mode or End-to-end Transparent mode.

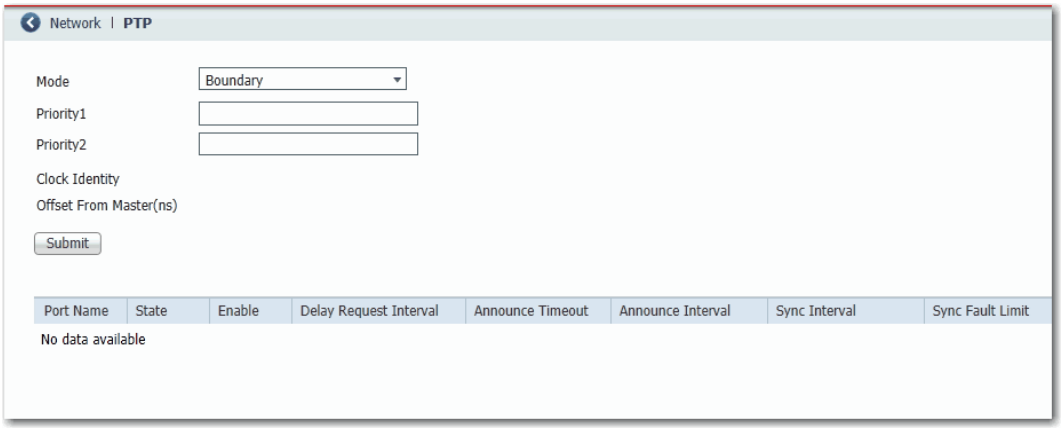


Table 16 - PTP Fields

Field	Description
Mode	Choose a PTP mode: • Boundary—Synchronizes all switch ports with the Grandmaster clock by using the IEEE 1588 V 2 Boundary clock mechanism. • End-to-End Transparent—Calculates and adds the switch delay into the PTP packet by using the IEEE 1588 V2 End-to-End Transparent clock mechanism. In this mode, all switch ports are PTP-enabled. In boundary mode, one or more switch ports can be PTP-enabled. You can enable or disable PTP on a per-port basis. • Forward (default)—Passes PTP packets through without interference.
Priority 1	The switch used to override the default criteria, such as clock quality or clock class, for the best master clock selection.
Priority 2	The switch used as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can give a specific switch priority over other identical switches. The range is from 0. . .255. A lower values take precedence. The default is 128.
Clock Identity	The clock source.
Offset from Master (ns)	The accuracy in nanoseconds from the Grandmaster clock.
Port Name	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch number (1), and the specific port number. For example: Fa1/1 is Fast Ethernet port 1 on the base switch.
State	(Boundary mode only). The synchronization state on the switch port with the parent or Grandmaster clock: • Listening—The switch port is waiting while a parent or Grandmaster clock is selected. • Pre-master—The switch port is transitioning to change to Master state. • Master—The switch is acting as a parent clock to the devices connected to that switch port. • Passive—The switch has detected a redundant path to a parent or Grandmaster clock. For example, two different switch ports claim the same parent or Grandmaster clock. To prevent a loop in the network, one of the ports changes to Passive state. • Uncalibrated—The switch port cannot synchronize with the parent or Grandmaster clock. • Slave—The switch port is connected to and synchronizing with the parent or Grandmaster clock. • Faulty—PTP is not operating properly on that switch port. • Disabled—PTP is not enabled on the switch port.
Enable	When at least one switch port is PTP-enabled, the Forward mode is selected by default: You can enable or disable PTP on a per-port basis.

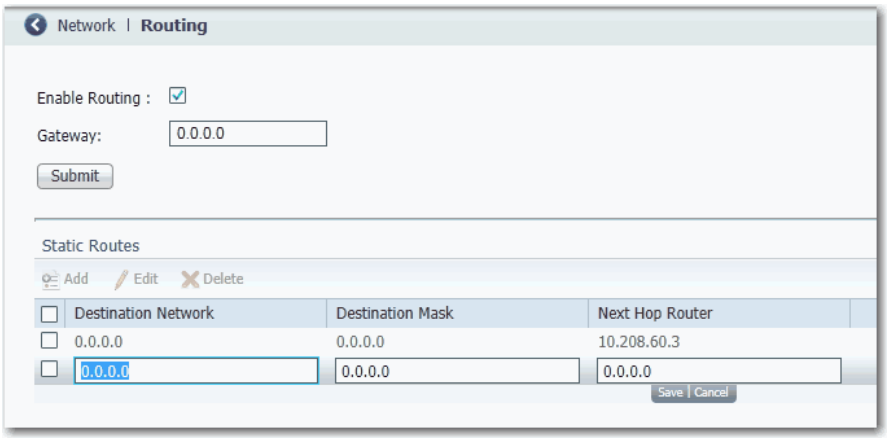
Table 16 - PTP Fields (continued)

Field	Description
Delay Request Interval	The time interval recommended to connected devices to send delay request messages when the switch port is in the master state: • **-1** means half second • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds • **5** means 32 seconds • **6** means 64 seconds The default is 5 (32 seconds).
Announce Timeout	The number of announce intervals that must pass without receipt of an announce message from the Grandmaster clock before the switch selects a new Grandmaster clock. The number can be from 2…10. The default is 3.
Announce Interval	The time interval for sending announce messages: • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds The default is 1 (2 seconds).
Sync Interval	The time interval for sending synchronization messages: • **-1** means half second • **0** means 1 second • **1** means 2 seconds The default is 0 (1 second).
Sync Fault Limit	The maximum clock offset before PTP attempts to reacquire synchronization. The value can be from 50…500,000,000 nanoseconds. The default is 50,000 nanoseconds. We recommend against setting the sync limit below the default (50,000 nanoseconds). Use values below 50,000 nanoseconds only in networks with a very-high-precision Grandmaster clock. These networks have a critical need to keep very sensitive devices synchronized.

Enable and Configure Routing

Before you can enable routing, you must reallocate switch memory for routing, as described on page 181.

To enable routing, from the Configure menu, choose Routing.



From the Routing window, you can enable connected routing only or both static and connected routing. When static routing is enabled, connected routing is enabled by default. For more information about these routing types, refer to Routing on page 113.

Enable Connected Routing Only

To enable connected routing only, check Enable Routing and click Submit.

No further configuration is required for connected routing.

Enable Both Static and Connected Routing

To enable both static and connected routing, follow these steps.

1. Check Enable Routing and click Submit.
2. Configure static route information as described below.

Field	Description
Destination Network	The IP address of the destination.
Destination Mask	The subnet mask of the destination.
Next Hop Router	The IP address of the router where this device will send the packets for the specified destination.

Configure STP

Spanning Tree Protocol (STP) modes include the following:

- Multiple Spanning Tree (MST) prevents network loops by enabling only one active path for traffic. MST also provides a redundant path if the active path becomes unavailable. This is the default STP mode.
- Per VLAN Spanning Tree Plus (PVST+) runs on each VLAN on the switch up to the maximum supported, ensuring loop-free path through the network.
- Rapid Per VLAN Spanning Tree Plus (RPVST+) immediately deletes dynamically learned MAC address entries upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC addresses.

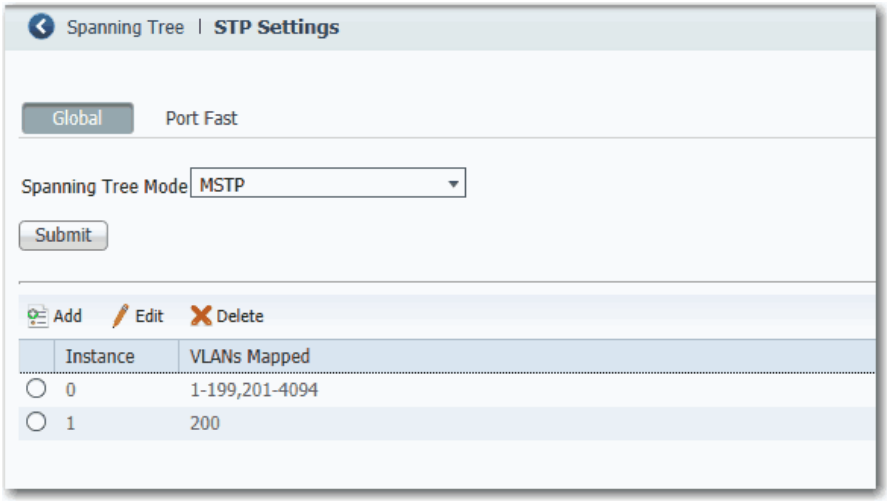
We recommend that you leave STP enabled to prevent network loops and provide a redundant path if the active path becomes unavailable.

IMPORTANT Disabling STP can affect connectivity to the network.

To configure Spanning Tree Protocol settings, from the Configure menu, choose STP.

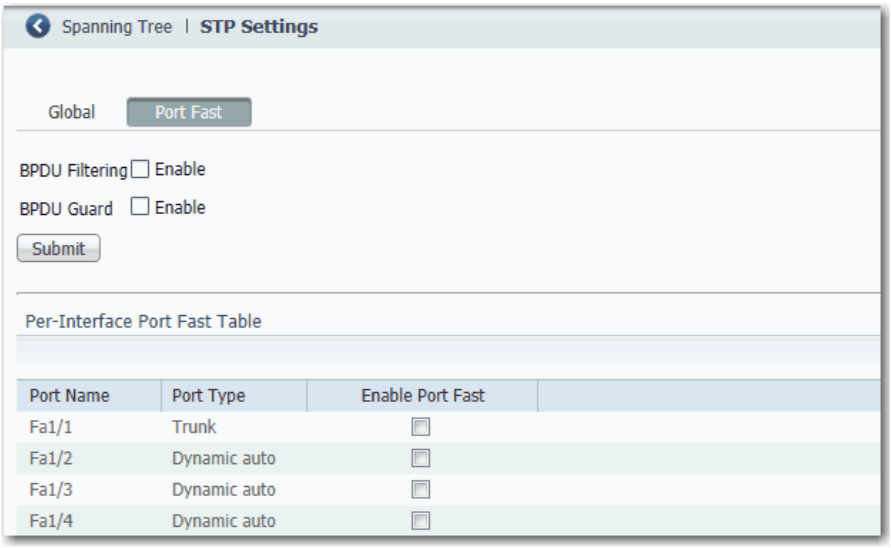
Global Settings

To choose the STP mode for the switch or to configure STP on individual VLANs, click the Global tab. On the Global tab, you can add, edit, or delete instances. If you choose PVST+ or Rapid PVST+ mode, you can enable or disable STP on each instance.



PortFast Settings

To enable PortFast and related features, click the PortFast tab. On the PortFast tab, you can change the way that STP is implemented on individual ports.



PortFast features are typically enabled only on access ports, which connect to devices such as personal computers, access points, and servers that are not expected to send bridge protocol data units (BPDUs). These features are typically not enabled on ports that connect to switches because spanning tree loops might occur.

BPDU Features

Switches exchange special frames called BPDUs to communicate network information, to track changes, and to create the STP topology. Because transmitted BPDUs reveal network information and received BPDUs can influence your STP topology, you might find it useful to enable BPDU Filtering and BPDU Guard on your access ports. These features prevent a rogue device from interfering with your STP topology. However, we recommend you use these features with caution:

- BPDU Filtering—This PortFast feature blocks all sending and receiving of BPDUs through all PortFast-enabled ports. This feature effectively disables STP on these ports and loops can result. If a BPDU is received, PortFast is disabled on the port and the global STP settings apply. To enable BPDU Filtering on all PortFast-enabled ports, check Enable.

- BPDU Guard—This PortFast feature shuts down a port if it receives a BPDU. To enable BPDU Guard on all Port Fast-enabled ports, check Enable.

Note that if you enable both of these features, BPDU Guard has no effect because BPDU Filtering prevents the port from receiving any BPDUs.

Per Interface PortFast Table

Spanning tree requires an interface to progress through the listening and learning states, to exchange information and establish a loop-free path before it can forward frames. On ports that connect to devices such as workstations and servers, you can allow an immediate connection. PortFast immediately transitions the port into STP forwarding mode upon linkup.

To enable PortFast on an interface and apply the selected BPDU features to the interface, select the interface, and then check Enable Port Fast.

Configure REP

To configure Resilient Ethernet Protocol (REP), from the Configure menu, choose REP.

To create a REP segment, set a segment ID and port type on the desired ports.

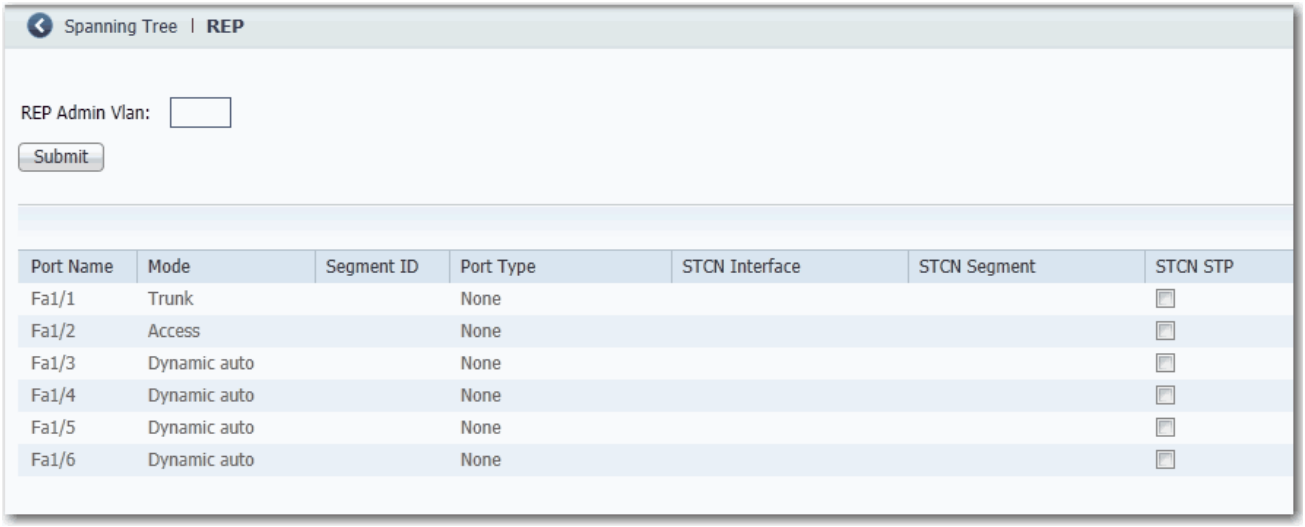


Table 17 - REP Fields

Field	Description
REP Admin VLAN	The administrative VLAN. The range is 2. . . 4094. The default is VLAN 1. REP ports are assigned to the same REP Admin VLAN. If the REP Admin VLAN changes, all REP ports are automatically assigned to the new REP Admin VLAN.
Port Name	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet).
Mode	The administrative mode. To set this mode, from the Configure menu, choose Port Settings.
Segment ID	The ID of the segment. The segment ID range is from 1. . . 1024. If no segment ID is set, REP is disabled.
Port Type	Each REP segment must have exactly two primary edge ports and may have secondary ports to use when a primary port fails. You can specify preferred primary and secondary ports. Configuring a port as preferred does not guarantee that it becomes the alternate port but gives it a slight edge among equal contenders. You also can indicate that a port is connected to switches that do not support REP. Choose one of these port types: • Edge—A secondary edge port that participates in VLAN load balancing. • Edge no-neighbor—A secondary edge port that is connected to a non-REP switch. • Edge no-neighbor preferred—A secondary edge port that is connected to a non-REP switch and is the preferred alternate port for VLAN load balancing. • Edge no-neighbor primary—A secondary edge port that always participates in VLAN load balancing in this REP segment and is connected to a non-REP switch. • Edge no-neighbor primary preferred—An edge port that always participates in VLAN load balancing in this REP segment, is connected to a non-REP switch, and is the preferred port for VLAN load balancing. • Edge preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing. • Edge primary—An edge port that always participates in VLAN load balancing in this REP segment. • Edge primary preferred—An edge port that always participates in VLAN load balancing in this REP segment and is the preferred port for VLAN load balancing. • None—This port is not part of the REP segment. The default is None. • Preferred—A secondary edge port that is the preferred alternate port for VLAN load balancing.
STCN Interface	Configure segment topology change notices (STCNs) for a port. The default is None. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN Segment	Configure STCNs to a segment ID. The default is a blank field. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN STP	Configure STCNs to an STP network. The default is cleared checkbox. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.

Configure NAT

To configure NAT, follow one of these procedures based on your application:

- Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

  For an example of this application, see Figure 4 on page 102.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

  For an example of this application, see Figure 5 on page 103.

IMPORTANT Set up all Smartport roles and VLANs before creating NAT instances.

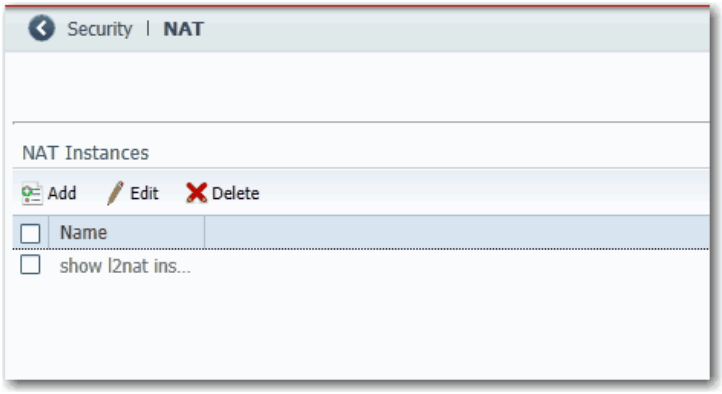
If you change a Smartport role or the native VLAN for a port associated with a NAT instance, you must reassign VLANs to the NAT instance.

IMPORTANT As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

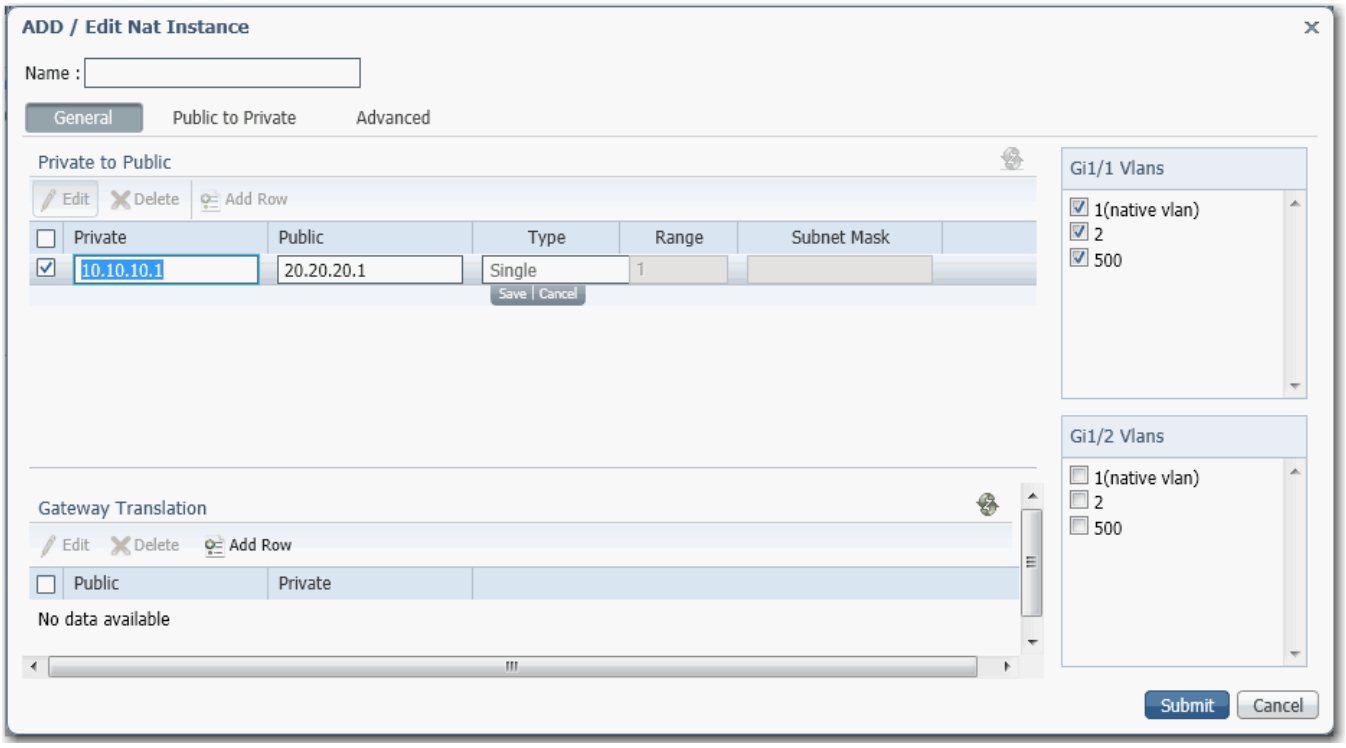
Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

To create a NAT instance for traffic routed through a Layer 3 switch or router, follow these steps.

1. From the Configure menu, choose NAT to display the NAT window.



2. Click Add to display the General tab of the Add/Edit NAT Instance window.



3. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

4. From the list of VLANs on the right, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 105.

5. In the Private to Public area, click Add Row, complete the fields, and click Save.

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Private IP Address</td><td colspan="2">Type a private IP address:
• To translate a single address, type the existing address for the device on the private subnet.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate as shown below.</td></tr>
<tr><td></td><td>Subnet Mask</td><td>Starting Private Subnet Address</td></tr>
<tr><td></td><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 192.168.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 192.168.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 192.168.1.0 or 192.168.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 192.168.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 192.168.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 192.168.1.16</td></tr>
<tr><td>Public IP Address</td><td colspan="2">Type a public IP address:
• To translate a single address, type a unique public address to represent the device.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.</td></tr>
<tr><td></td><td>Subnet Mask</td><td>Starting Public Subnet Address</td></tr>
<tr><td></td><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 10.200.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 10.200.1.0.</td></tr>
<tr><td></td><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 10.200.1.0 or 10.200.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 10.200.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 10.200.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 10.200.1.16</td></tr>
</table>

Field	Description
Type	Choose one of these values: • Single—Translate a single address. • Range—Translate a range of addresses. • Subnet—Translate all of the addresses in the private subnet or a portion of the private subnet.
Range	Type the number of addresses to translate. This field is available only if you choose Range in the Type field. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Subnet Mask	Type the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry) – 255.255.255.192 (provides 64 addresses per translation entry) – 255.255.255.224 (provides 32 addresses per translation entry) – 255.255.255.240 (provides 16 addresses per translation entry)

6. In the Gateway Translation area, click Add Row, complete the fields, and click Save.

   The gateway translation enables devices on the public subnet to communicate with devices on the private subnet.

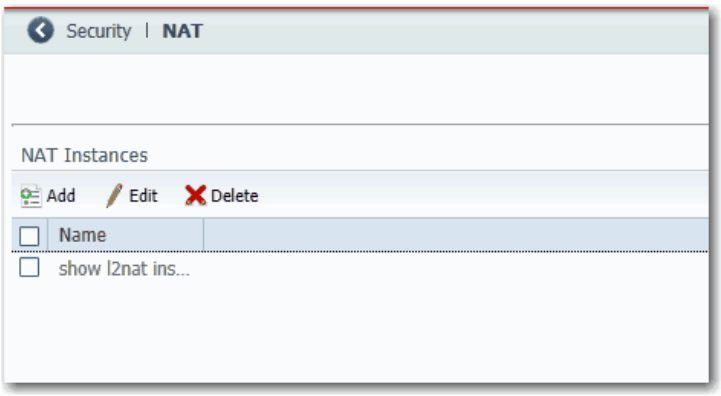
Field	Description
Public	Type the default gateway address of the Layer 3 switch or router connected to the switch's uplink port.
Private	Type a unique IP address to represent the Layer 3 switch or router on the private network.

7. (Optional). To configure traffic permits and packet fixups, proceed to Configure Traffic Permits and Fixups on page 161.
8. Click Submit.

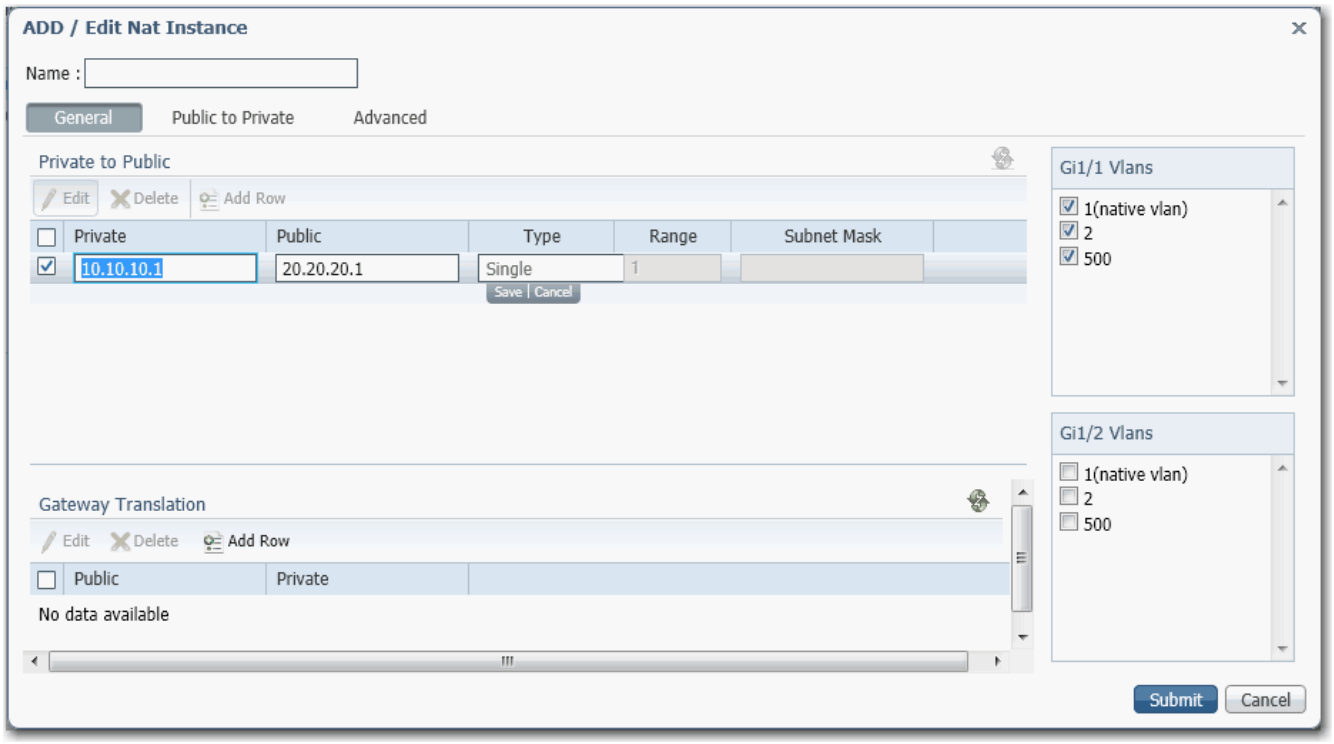
Create NAT Instances for Traffic Routed through a Layer 2 Switch

To create a NAT instance for traffic routed through a Layer 2 switch, follow these steps.

1. From the Configure menu, choose NAT to display the NAT window.



2. Click Add to display the General tab of the Add/Edit NAT Instance window.



3. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

4. From the list of VLANs on the right, check the checkbox next to each VLAN to assign to the instance.

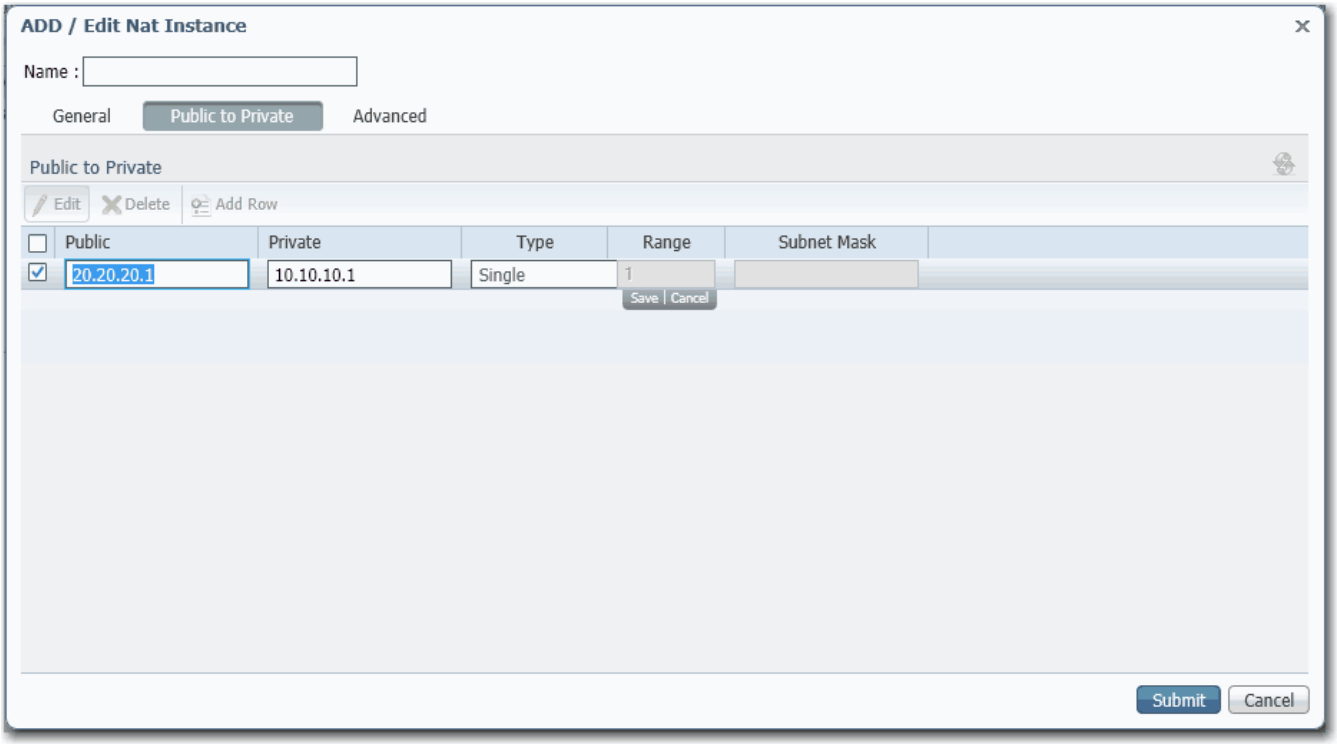
   For more information about VLAN assignments, see page 105.

5. In the Private to Public area, click Add Row, complete the fields, and click Save.

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Private IP Address</td><td colspan="2">Type a private IP address:
• To translate a single address, type the existing address for the device on the private subnet.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate as shown below.</td></tr>
<tr><td></td><td>Subnet Mask</td><td>Starting Private Subnet Address</td></tr>
<tr><td></td><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 192.168.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 192.168.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 192.168.1.0 or 192.168.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 192.168.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 192.168.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 192.168.1.16</td></tr>
<tr><td>Public IP Address</td><td colspan="2">Type a public IP address:
• To translate a single address, type a unique public address to represent the device.
• To translate a range of addresses, type the first address in the range of sequential addresses.
• To translate addresses in a subnet, type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.</td></tr>
<tr><td></td><td>Subnet Mask</td><td>Starting Public Subnet Address</td></tr>
<tr><td></td><td>255.255.0.0</td><td>The last two octets must end in 0.
EXAMPLE: 10.200.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>The last octet must end in 0.
EXAMPLE: 10.200.1.0.</td></tr>
<tr><td></td><td>255.255.255.128</td><td>The last octet must end in 0 or 128.
EXAMPLE: 10.200.1.0 or 10.200.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>The last octet must in one of the following: 0, 64, 128, 192.
EXAMPLE: 10.200.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224.
EXAMPLE: 10.200.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXAMPLE: 10.200.1.16</td></tr>
</table>

Field	Description
Type	Choose one of these values: • Single—Translate a single address. • Range—Translate a range of addresses. • Subnet—Translate all of the addresses in the private subnet or a portion of the private subnet.
Range	Type the number of addresses to translate. This field is available only if you choose Range in the Type field. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Subnet Mask	Type the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)

6. Click the Public to Private tab.



7. Click Add Row, complete the fields, and click Save.

Field	Description	
Public IP Address	Type a public IP address: • To translate a single address, type the existing address for the device on the public subnet. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type the existing starting address for the range of devices on the public subnet. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0.
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16
Private IP Address	Type a private IP address: • To translate a single address, type a unique private address to represent the device. • To translate a range of addresses, type the first address in the range of sequential addresses. • To translate addresses in a subnet, type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16

Field	Description
Type	Choose one of these values: • Single—Translate a single address. • Range—Translate a range of addresses. • Subnet—Translate all of the addresses in the public subnet or a portion of the public subnet.
Range	Type the number of addresses to translate. This field is available only if you choose Range in the Type field. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Subnet Mask	Type the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)

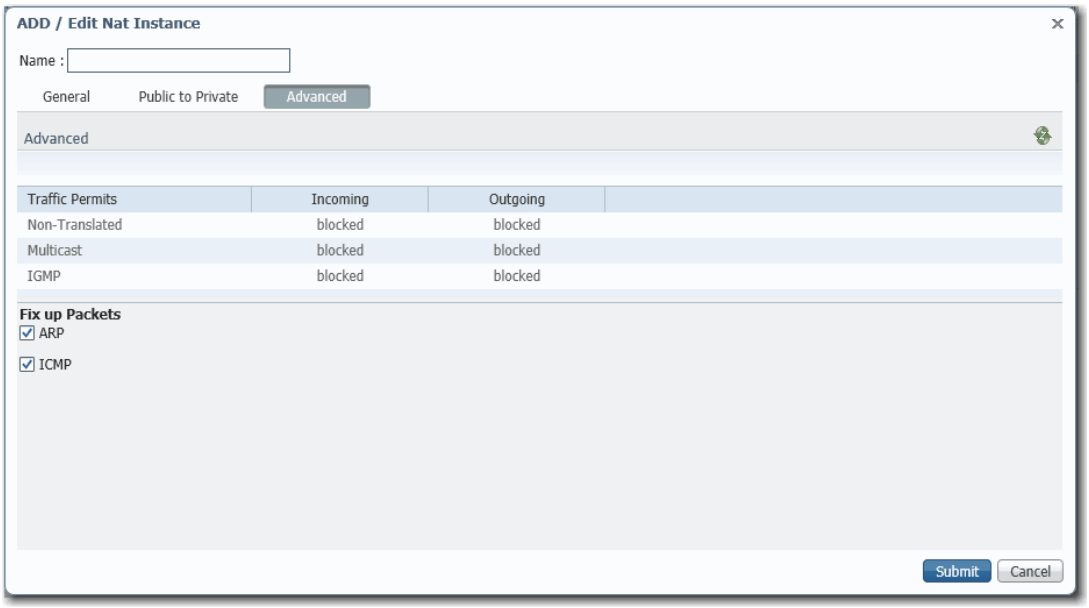
8. (Optional). To configure traffic permits and packet fixups, proceed to Configure Traffic Permits and Fixups below.
9. On the NAT window, click Submit.

Configure Traffic Permits and Fixups

Use caution when configuring traffic permits and fixups. We recommend you use the default values.

To configure traffic permits or fixups, follow these steps.

1. Click the Advanced tab.



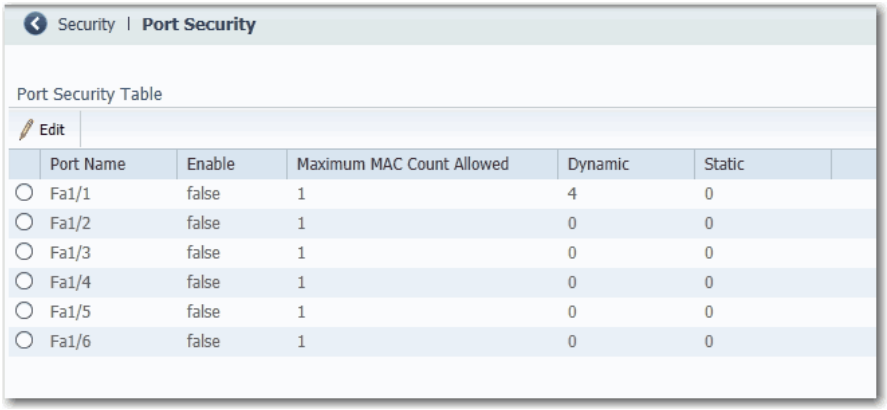
2. Choose one of these options for incoming and outgoing packets that are not handled by NAT:
   - Pass-through—Permit the packets to pass across the NAT boundary.
   - Blocked—Drop the packets.
3. In the Fix up Packets area, check or clear the checkboxes to enable or disable fixups for ARP and ICMP.

   By default, fixups are enabled for both ARP and ICMP.
4. Click Submit.

Configure Port Security

Configure port security to limit the MAC addresses (MAC IDs) that can access a given port. Port security is based on the number of MAC addresses supported (none of which are statically defined). Static port security lets you specify whether MAC addresses are auto-learned or manually defined.

To configure port security, from the Configure menu, choose Port Security.



Port security limits and identifies the MAC addresses of devices that can send traffic through the switch port. The switch port does not forward traffic from devices outside the defined group of devices. A security violation occurs when any of the following conditions occur:

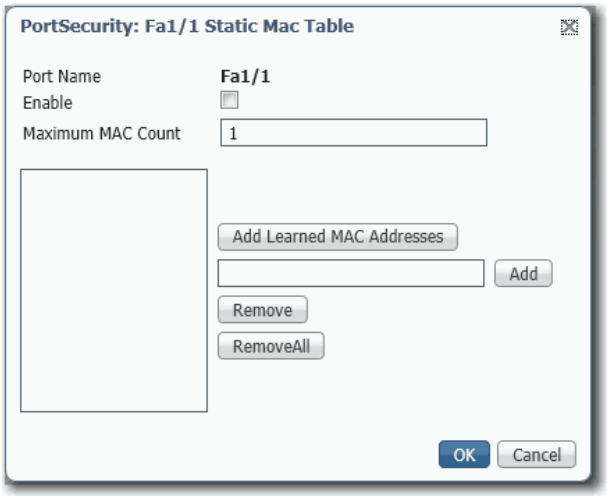
- A device, which has a MAC address different from any identified secure MAC addresses, attempts to access the switch port.
- The number of MAC addresses on the port exceeds the maximum number supported on the port.

Port security supports multiple security levels:

- The ability to define the number of devices that are connected to a given port. These are assigned on a first-come, first-served basis and time out after a certain period of inactivity.
- The ability to easily store the existing MAC Address configuration by selecting Add Learned MAC Addresses on the Static MAC Address Table.
- The ability to manually add and remove MAC Addresses on a per port basis.

To change the Static MAC Addresses table for a port, do the following:

1. Click the radio button next to the port to configure.
2. Click Edit.
3. Clear or check the Enable checkbox.
4. Configure MAC addresses as follows:
   - To add the existing MAC addresses of devices currently connected to a port, click Add Learned MAC Addresses.
   - To add a specific MAC address to the table, type a MAC address in the format fields and click Add.
   - To remove a MAC address from the table, select the MAC address and click Remove.
   - To clear the MAC address table, click Remove All.



5. Click OK.

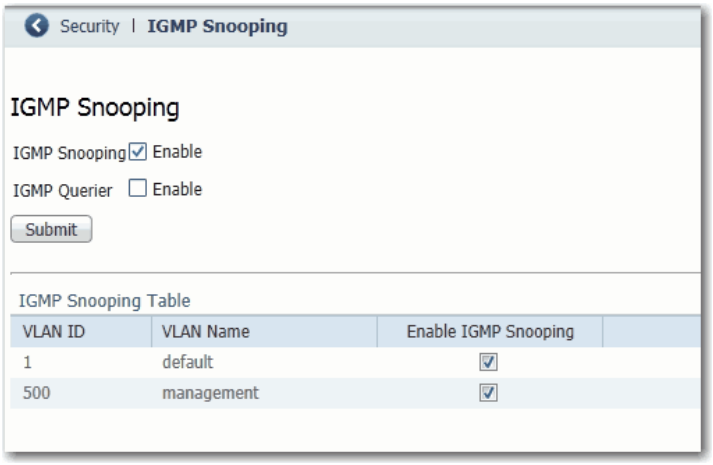
Configure IGMP Snooping

Internet Group Management Protocol (IGMP) snooping reduces duplicate and excess traffic on the network by forwarding IP multicast traffic to specific switch ports rather than by flooding all ports.

With IGMP snooping, ports that are members of only specific IP multicast groups receive multicast messages. The result is a more efficient use of bandwidth.

To configure IGMP snooping, from the Configure menu, choose IGMP Snooping:

- To enable IGMP Snooping for all VLAN IDs, check Enable next to IGMP Snooping.
- To enable IGMP Querier for all VLAN IDs, check Enable next to IGMP Querier.
- To enable or disable IGMP snooping on a VLAN, select the VLAN and check or clear the Enable IGMP Snooping checkbox.

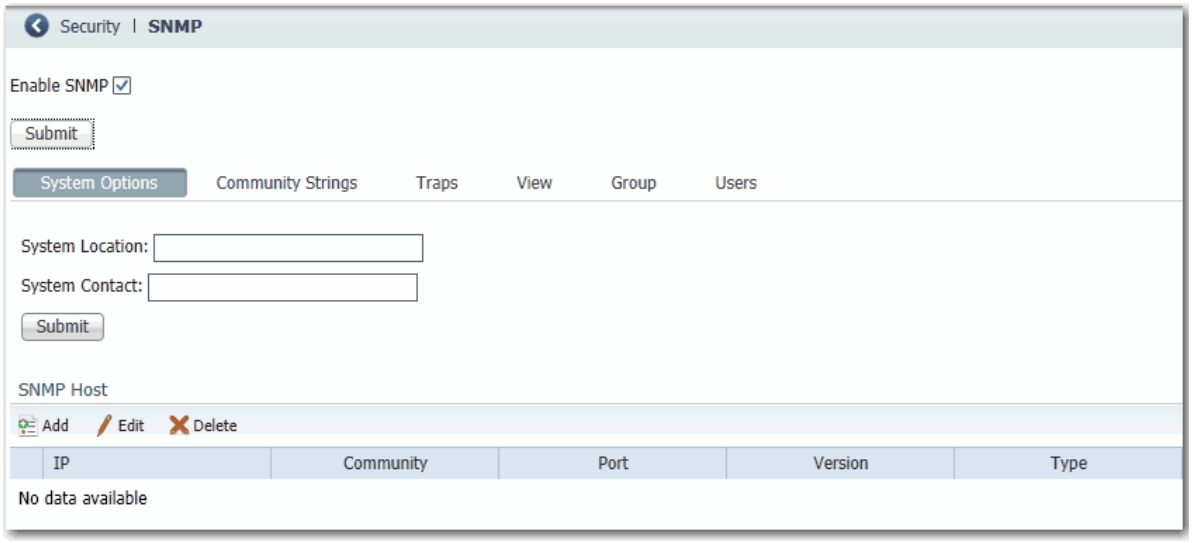


Configure SNMP

Enable SNMP if you plan to have the switch managed through another network management application. By default, SNMP is disabled.

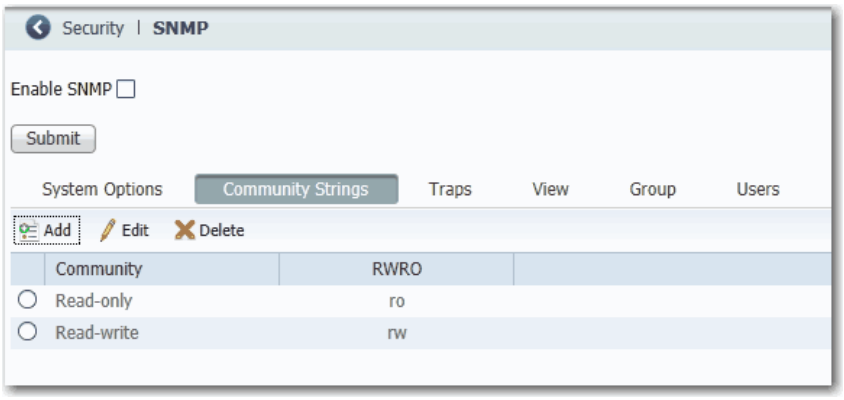
Other general SNMP settings include the name of the switch or the network administrator and the switch location. The system name and the system contact information appear in the Switch Information area on the Dashboard.

To configure SNMP, from the Configure menu, choose SNMP.



Community strings are passwords to the switch Management Information Base (MIB). You can create community strings that provide a remote manager read-only or read-write access to the switch.

To create, modify, and delete community strings, click the Community Strings tab.



A read-only community string enables the switch to validate Get (read-only) requests from a network management station. If you set the SNMP read community, users can access MIB objects, but cannot change them.

A read-write community string enables the switch to validate Set (read-write) requests from a network management station.

Use SNMP Management Applications

You can use SNMP management applications such as IntraVue or HP OpenView to configure and manage the switch. Refer to SNMP on page 111 for more information.

Configure Alarm Settings

The switch software monitors conditions on a per port or a global basis. If the conditions do not match the set parameters, an alarm or a system message is triggered. By default, the switch sends the system messages to a logging facility. You can configure the switch to send SNMP traps to an SNMP server. You also can configure the switch to trigger an external alarm device by using the two independent alarm relays.

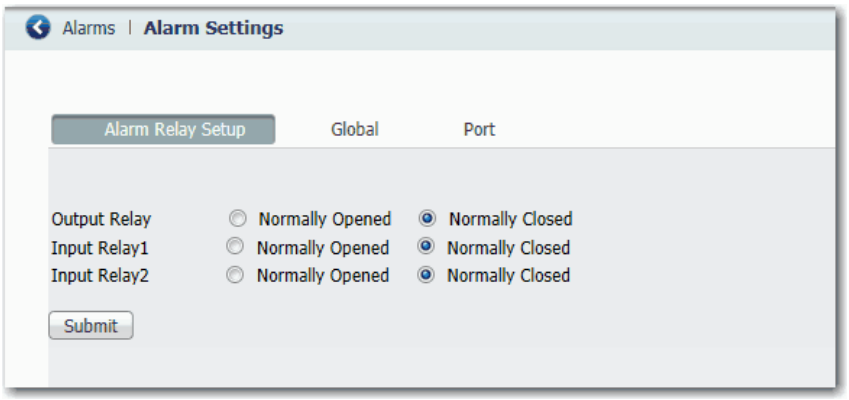
Alarm Relay Settings

You can configure the switch to trigger an external alarm device. The switch supports two alarm inputs and one alarm output. The switch software is configured to detect faults which are used to energize the relay coil and change the state on both of the relay contacts. Normally open contacts close and normally closed contacts open.

To configure alarm relay settings, from the Configure menu, choose Alarm Settings.

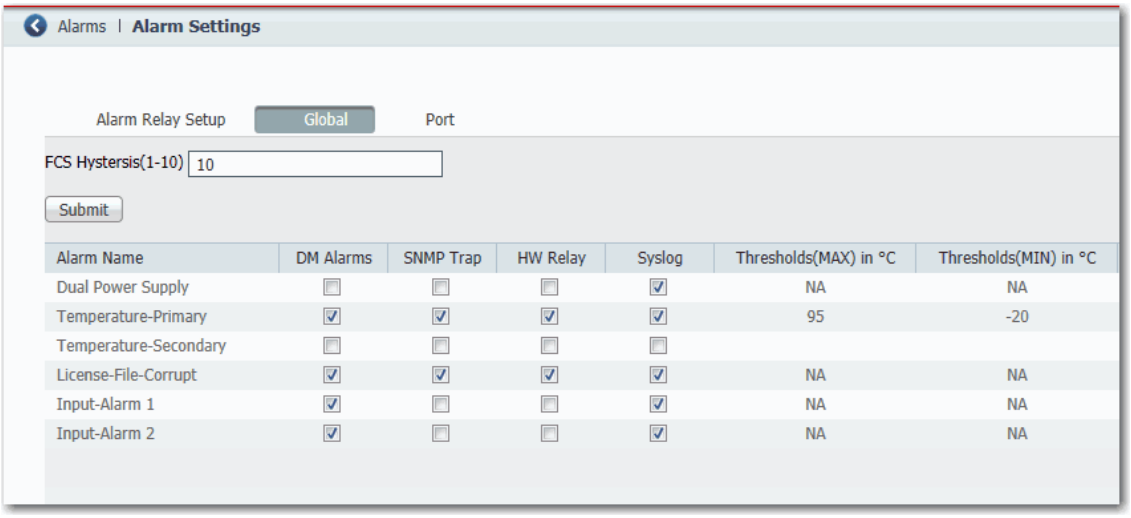
On the Alarm Relay Setup tab, click one of these options for each type of alarm relay:

- Normally Opened—The normal condition is that no current flows through the contact. The alarm is generated when current flows.
- Normally Closed—The normal condition has current flowing through the contact. The alarm is generated when the current stops flowing.



Global Alarms

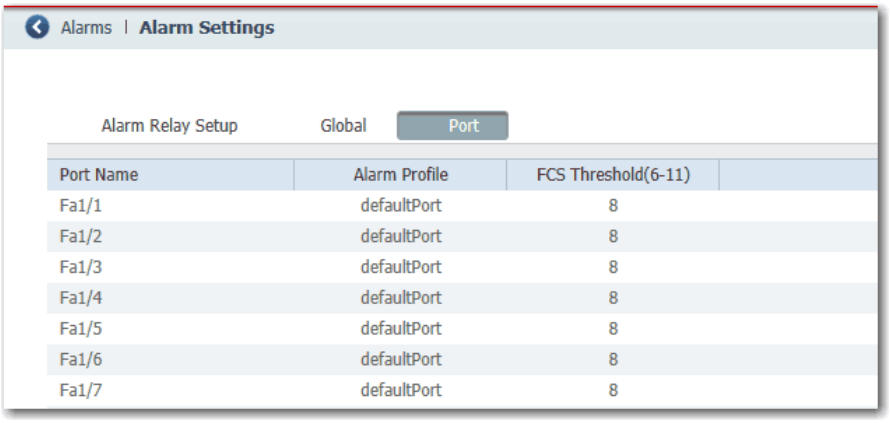
To configure global alarms, also known as facility alarms, from the Configure menu, choose Alarm Settings and click the Global tab.



Field	Description
FCS Hysteresis (1-10)	The frame check sequence (FCS) error hysteresis threshold is used to determine when an alarm condition is cleared. This value is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8 percent. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for global settings are 1…10. This setting also can be configured on an individual port by clicking the Port tab.
Alarm Name	These types of alarms can be enabled or disabled: • Dual Power Supply—The switch monitors DC power supply levels. If the system is configured to operate in a dual power mode, an alarm is triggered if a power supply fails or is missing. The alarm is automatically cleared when the power supplies are present or working. You can configure the power supply alarm to be connected to the hardware relays. • Temperature-Primary—These alarms are triggered when the system temperature is higher or lower than the configured thresholds. By default, the primary temperature alarm is associated with the major relay. • Temperature-Secondary—These alarms are triggered when the system temperature is higher or lower than the configured thresholds. • License-File-Corrupt—An alarm is triggered when the license file is corrupt. • Input-Alarm 1—An alarm is triggered based on an external input alarm. • Input-Alarm 2—An alarm is triggered based on an external input alarm.
DM Alarms	Alarm information appears on the dashboard of the Device Manager Web interface.
SNMP Trap	Alarm traps will be sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	The switch's alarm relay is triggered, sending a fault signal to a connected external alarm device, such as a bell, light, or other signaling device that you have configured.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.
Thresholds (MAX) in °C	The maximum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.
Thresholds (MIN) in °C	The minimum temperature threshold for the corresponding Temperature-Primary or Temperature-Secondary alarm, if enabled.

Port Alarms

To create alarm profiles for individual ports, from the Configure menu, choose Alarm Settings and click the Port tab.



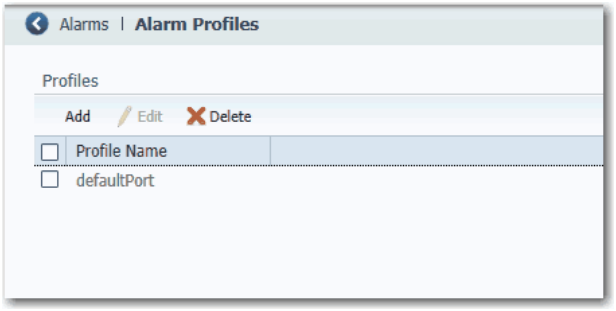
For each port, choose an Alarm Profile and set the FCS threshold. The frame check sequence (FCS) error hysteresis threshold is expressed as a percentage of fluctuation from the FCS bit error rate. The default setting is 8 percent. You can adjust the percentage to prevent toggling the alarm condition when the FCS bit error rate fluctuates near the configured bit error rate. Valid percentages for port settings are 6...11.

Configure Alarm Profiles

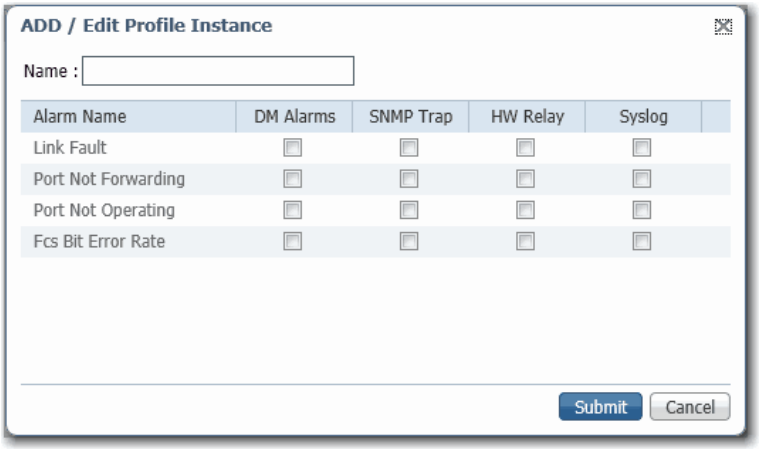
You can use alarm profiles to apply a group of alarm settings to multiple interfaces. These alarm profiles are created for you:

- defaultPort
- ab-alarm (created during Express Setup)

To create, modify, or delete alarm profiles, from the Configure menu, choose Alarm Profiles.



On the Add/Edit Profile Instance window, you can configure the alarms and actions for an alarm profile.



Field	Description
Name	A unique name for the alarm profile.
Alarm Name	These types of alarms can trigger an action.
DM Alarms	Alarm information appears on the dashboard of the Device Manager Web interface.
SNMP Trap	Alarm traps will be sent to an SNMP server, if SNMP is enabled on the Configure > Security > SNMP window.
HW Relay	The switch's alarm relay is triggered, sending a fault signal to a connected external alarm device, such as a bell, light, or other signaling device that you have configured.
Syslog	Alarm traps are recorded in the syslog. You can view the syslog on the Monitor > Syslog window.

Monitor Trends

You can view historical data to help you to analyze traffic patterns and to identify problems. Data can be displayed in increments of seconds, minutes, hours, or days.

To view the data in a table, click the Grid Mode button below the area. To display a chart, click the Chart Mode button. Use the 60s, 1h, 1 d, and 1 w links to display the data in increments of 60 seconds, 1 hour, 1 day, or 1 week.

To monitor trends, from the Monitor menu, choose Trends.

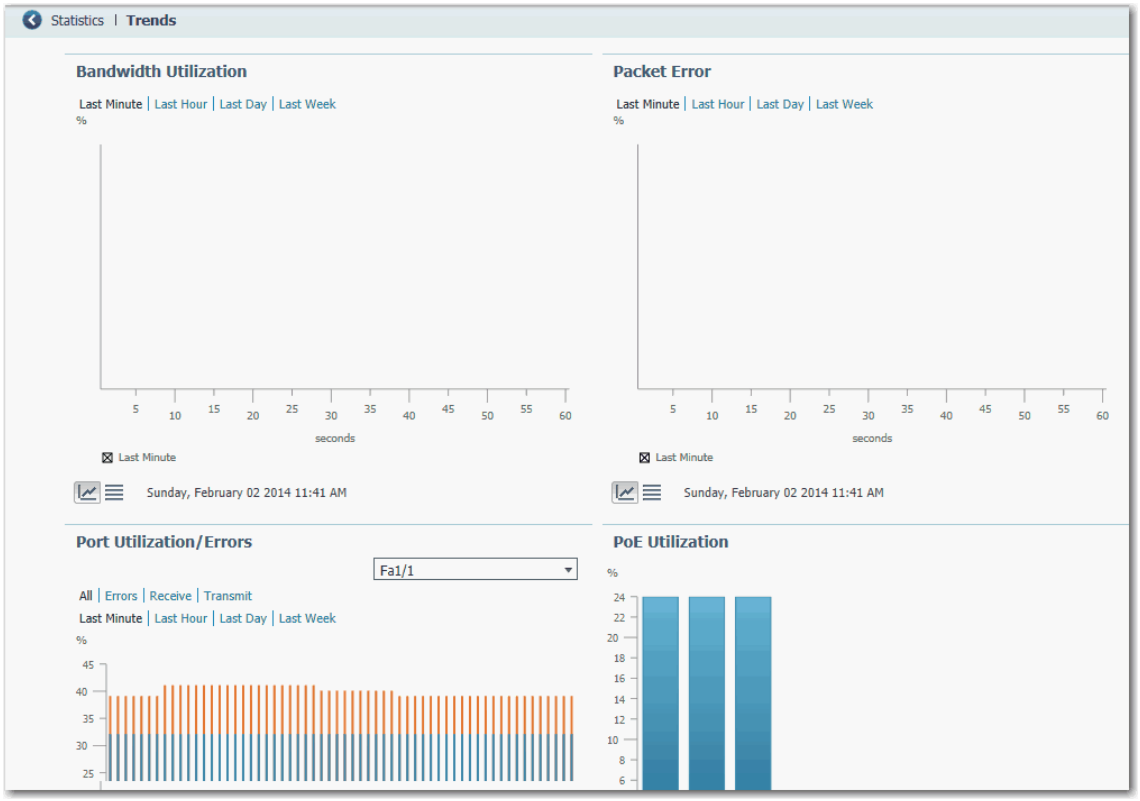

Statistics | Trends
Bandwidth Utilization
Last Minute | Last Hour | Last Day | Last Week
%
5 10 15 20 25 30 35 40 45 50 55 60
seconds
Last Minute
Sunday, February 02 2014 11:41 AM
Packet Error
Last Minute | Last Hour | Last Day | Last Week
%
5 10 15 20 25 30 35 40 45 50 55 60
seconds
Last Minute
Sunday, February 02 2014 11:41 AM
Port Utilization/Errors
Fa1/1
All | Errors | Receive | Transmit
Last Minute | Last Hour | Last Day | Last Week
%
45 40 35 30 25
PoE Utilization
%
24 22 20 18 16 14 12 10 8 6

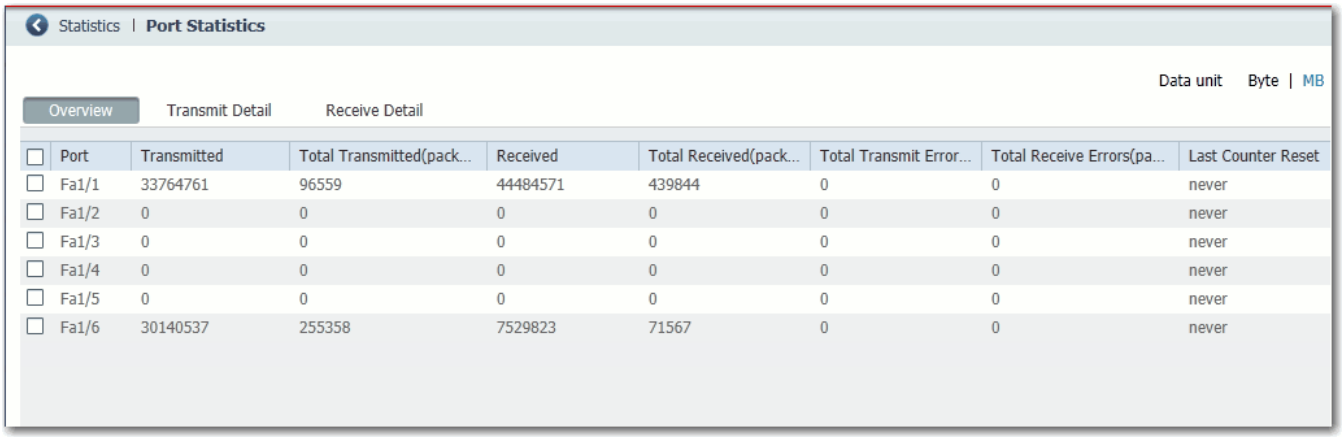
Table 18 - Trends Graphs

Graph	Description
Bandwidth Utilization	The Bandwidth Utilization graph indicates the percentage of the available bandwidth that was used. The graph can show the bandwidth usage patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). This graph also marks the highest peak reached. The default is 60 seconds. You can use this data to determine when network usage is high or low.
Packet Error	The Packet Error graph shows the percentage of packet errors collected over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. Use this graph to audit the affects that connected devices have on the switch performance or the network. For example, if you suspect that a connected device is sending error packets, you can verify if the data on the graph changes when you disconnect and reconnect the suspected device.
Port Utilization/Errors	The Port Utilization/Errors graph show the usage patterns of a specific port over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. To display the trends for a specific port, choose a port from the Port list. Use these graphs to observe the performance of a specific port. For example, if a network user is having intermittent network connectivity, use the Port Utilization graph to observe the traffic patterns on the port to which the user's personal computer is connected, and use the Port Errors graph to see if the port is receiving or sending error packets.
PoE Utilization	For PoE switches, the PoE Utilization graph shows the power that is allocated to the connected devices.

Monitor Port Statistics

You can view statistics for data sent and received by the switch ports since the switch was last powered on, was restarted, or since the statistics were last cleared.

To monitor port statistics, from the Monitor menu, choose Port Statistics. See the Device Manager Web interface online help for additional information.



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

The types of port statistics collected and displayed are grouped under these tabs on the Port Statistics window on the Device Manager Web interface:

- Overview tab—Use this tab to display the specific numbers of error packets received on and sent from the port, which is a level of detail that is not available from the Dashboard graphs.

  The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity.

- Transmit Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets sent from each port
  – Detailed statistics of errors sent to each port

  If a port is sending an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal or if it could mean a problem.

- Receive Detail tab—Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets received on each port
  – Detailed statistics of errors received on each port

  If a port is receiving an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal for the connected device or if it could mean a problem.

Monitor NAT Statistics

You can monitor these types of NAT statistics:

- Global statistics for all instances
- Statistics per instance
- Detailed private translations per instance
- Detailed public translations per instance

To display the NAT Statistics window, from the Monitor menu, choose NAT Statistics.

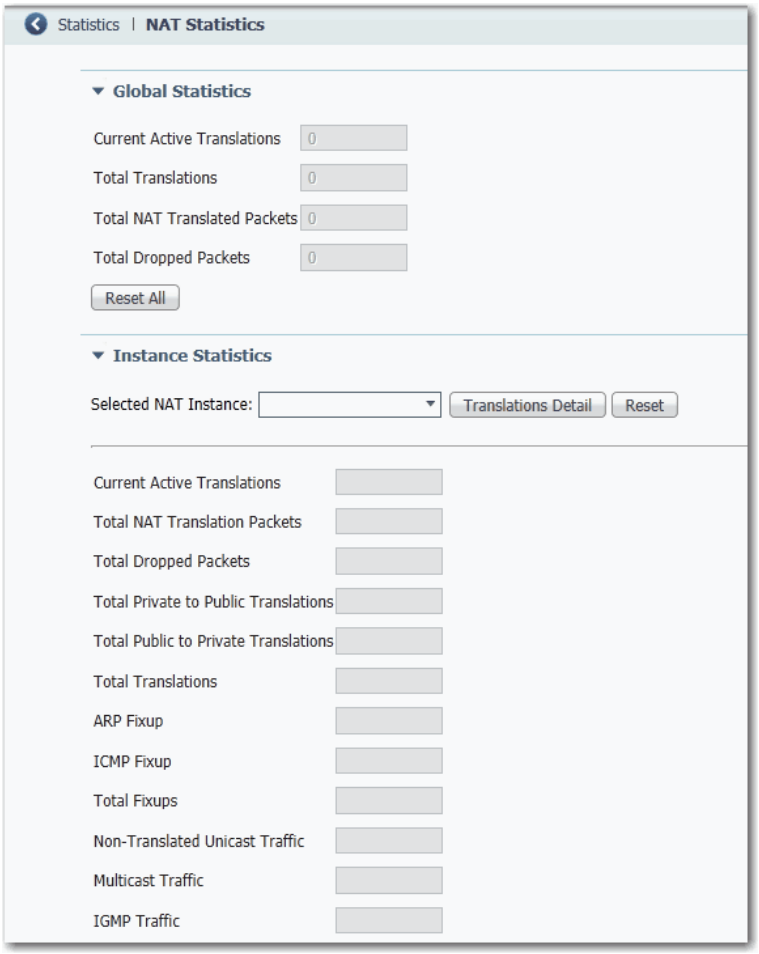


Table 19 - NAT Global Statistics

Field	Description
Current Active Translations	The number of IP addresses that have been translated within the last 90 seconds across all NAT instances.
Total Translations	The total number of translations across all NAT instances.
Total NAT Translated Packets	The total number of packets across all NAT instances.
Total Dropped Packets	The total number of packets that have been dropped across all NAT instances.

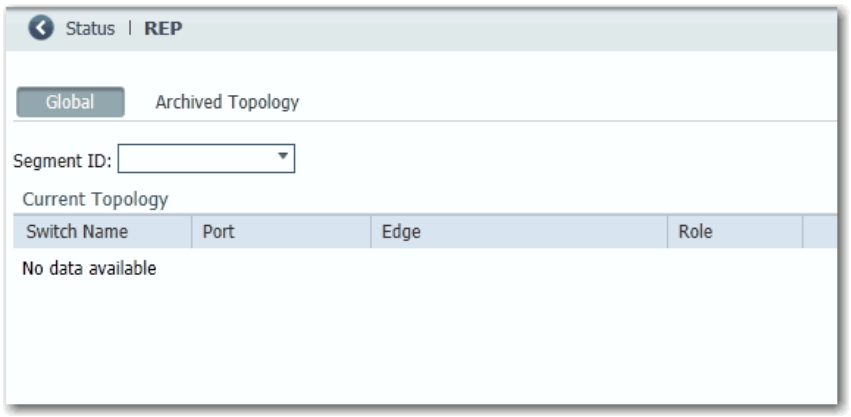
Table 20 - Instance Statistics

Field	Description
Selected Instance	From the pull-down menu, choose the instance for which to view statistics.
Current Active Translations	The number of translations that have occurred within the last 90 seconds for the instance.
Total NAT Translated Packets	The total number of packets that have been translated for the instance.
Total Dropped Packets	The total number of packets that have been dropped for the instance.
Total Private to Public Address Translations	The total number of translations configured for devices on the private subnet.
Total Public to Private Address Translations	The total number of translations configured for devices on the public subnet.
Total Translations	The total number of translations configured for the instance.
ARP Fixup	The number of ARP packets that have been fixed up for the instance.
ICMP Fixup	The number of ICMP packets that have been fixed up for the instance.
Total Fixups	The total number of ARP and ICMP packets that have been fixed up for the instance.
Non-Translated Unicast Traffic	The number of packets with untranslated unicast traffic for the instance.
Multicast Traffic	The number of packets with multicast traffic for the instance.
IGMP Traffic	The number of packets with IGMP traffic for the instance.

Monitor REP Topology

To review the REP topology for one or all network segments, from the Monitor menu, choose REP.

To display an archived REP topology, click the Archived Topology tab and then select the segment ID.



Monitor CIP Status

Common Industrial Protocol (CIP) is an application layer messaging protocol used by various industrial automation and control devices to communicate as part of a control system. CIP is the application layer for the EtherNet/IP network. Stratix switches contain an EtherNet/IP server that enables the switch to be part of the industrial automation and control system for basic management and monitoring.

The CIP Status window displays information about CIP status (Overview field) and statistics (Request Details field) since the switch was last powered on, was restarted, or the counters were last reset.

To troubleshoot an issue, reset the CIP counters, and see if the counters show that the issue still exists.

IMPORTANT Except for Active Multicast Groups, all other categories are related to the CIP server in the switch, that is, pertaining to CIP traffic specifically directed to the switch as a CIP target device. They do not refer to CIP (EtherNet/IP) traffic flowing through the switch among various CIP controllers, HMI devices, configuration tools, or other CIP target devices, such as drives, I/O modules, motor starters, sensors, and valves.

To monitor CIP status, from the Monitor menu, choose CIP Status.

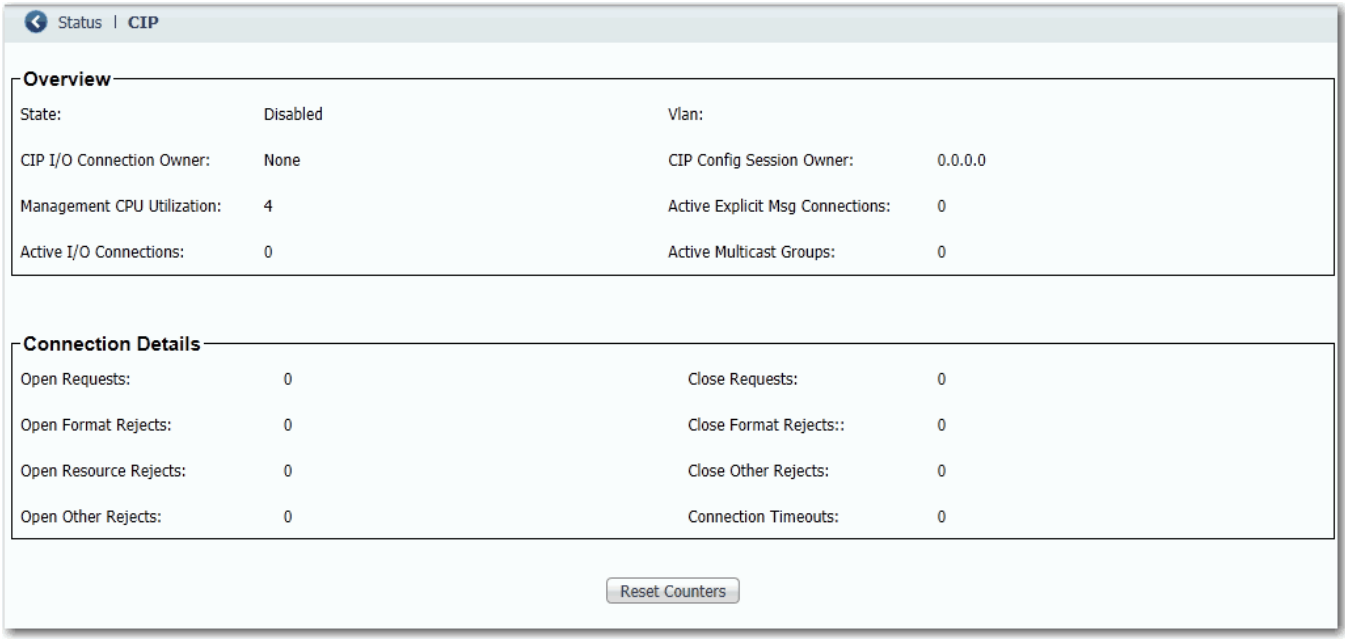


Table 21 - CIP Status Fields

Field	Description
Overview	
State	The state of the CIP connection (Enabled or Disabled).
Vlan	The VLAN ID.
CIP I/O Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent and received.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Management CPU Utilization (%)	Percentage of the Management CPU used for management functions. Switch functions have dedicated ASICs that are not impacted by management functions.
Active Explicit Msg Connections	The number of active, explicit messaging connections to the switch as a target.
Active I/O Connections	The number of active I/O connections with the switch as a target.
Active Multicast Groups	The number of multicast groups, including CIP multicast groups flowing through the switch.
Connection Details	
Open Requests	The number of Forward Open requests received by the switch to establish a connection with the switch.
Close Requests	The number of Forward Close requests received by the switch after a connection was successfully established with the switch.
Open Format Rejects	The number of Forward Open requests directed to the switch that failed because the request is not in the proper format.
Close Format Rejects	The number of Forward Close requests directed to the switch that failed because the request is not in the proper format.
Open Resource Rejects	The number of Forward Open requests that failed to establish a new connection for reasons such as insufficient memory.
Close Other Rejects	The number of Forward Close requests that failed for reasons such as incompatible electronic keying.
Open Other Rejects	The number of Forward Open requests that failed for reasons such as incompatible electronic keying.
Connection Timeouts	The number of CIP connections that timed out due to inactivity.

Diagnose Cabling Problems

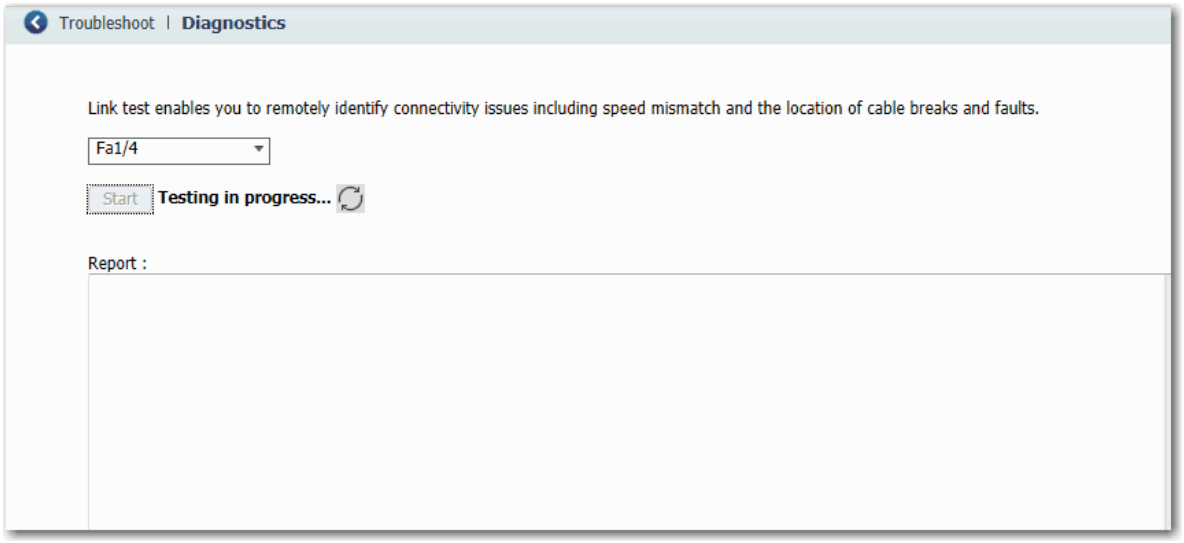
Use the Diagnostics window to run the Broken Wire Detection test, which uses Time Domain Reflectometry (TDR) detection to identify, diagnose, and resolve cabling problems. TDR detection is supported on copper Ethernet 10/100 and 10/100/1000 ports. TDR is not supported on small form-factor pluggable (SFP) module ports.

The link test can interrupt traffic between the port and the connected device. Only run the test on a port that has a suspected problem. Before running the link test, use the Front Panel view, the Port Status, and the Port Statistics windows to gather information about a potential problem.

IMPORTANT To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type, as described in Configure Port Settings on page 132.

To diagnose cabling, from the Monitor menu, choose Diagnostics.

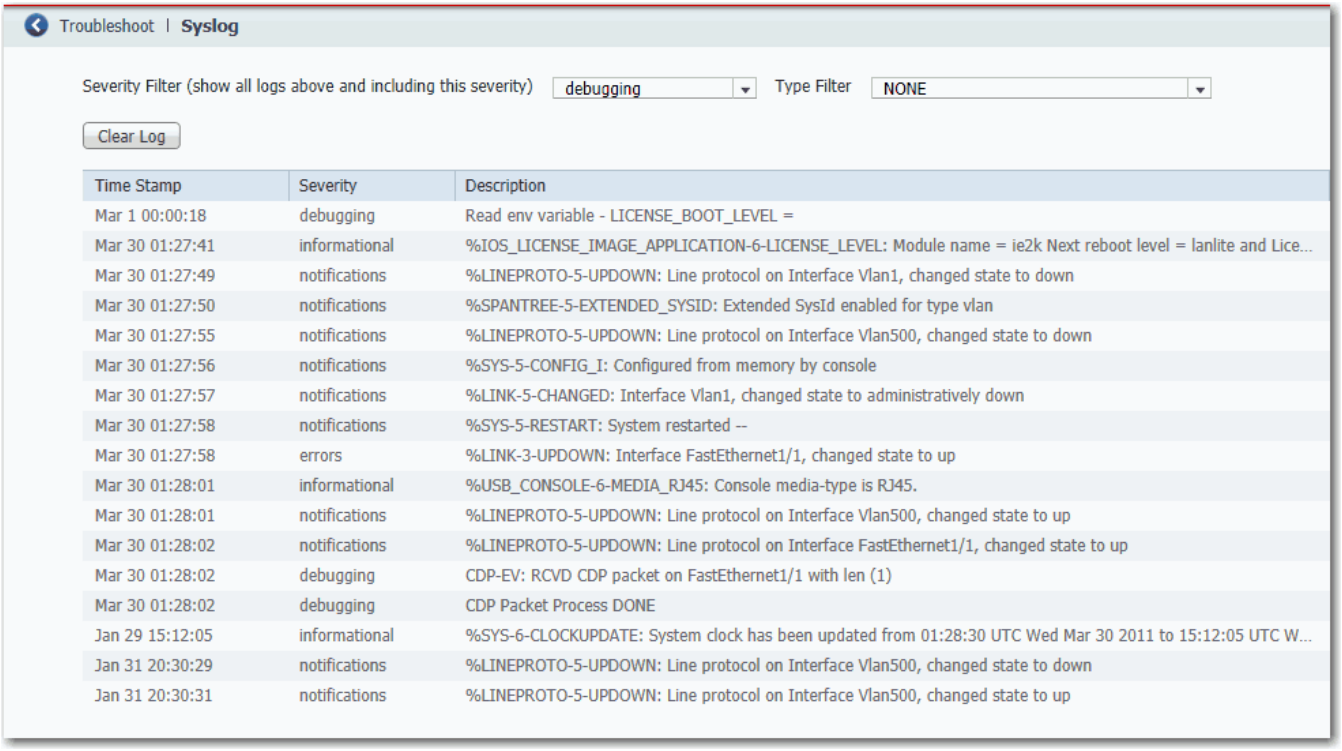
To run a test, select a port and then click Start.


Troubleshoot | Diagnostics
Link test enables you to remotely identify connectivity issues including speed mismatch and the location of cable breaks and faults.
Fa1/4
Start
Testing in progress...
Report :

View System Log Messages

The system log displays events that occurred on the device and its ports, based on the Alarm Settings you configure on the Configure > Alarm Settings window.

To view system log messages, from the Monitor menu, choose Syslog.


Troubleshoot | Syslog
Severity Filter (show all logs above and including this severity)
debugging
Type Filter
NONE
Clear Log
Time Stamp
Severity
Description
Mar 1 00:00:18 debugging Read env variable - LICENSE_BOOT_LEVEL =
Mar 30 01:27:41 informational %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = ie2k Next reboot level = lanlite and Lice...
Mar 30 01:27:49 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Mar 30 01:27:50 notifications %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
Mar 30 01:27:55 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to down
Mar 30 01:27:56 notifications %SYS-5-CONFIG_I: Configured from memory by console
Mar 30 01:27:57 notifications %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
Mar 30 01:27:58 notifications %SYS-5-RESTART: System restarted --
Mar 30 01:27:58 errors %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
Mar 30 01:28:01 informational %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
Mar 30 01:28:01 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to up
Mar 30 01:28:02 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
Mar 30 01:28:02 debugging CDP-EV: RCVD CDP packet on FastEthernet1/1 with len (1)
Mar 30 01:28:02 debugging CDP Packet Process DONE
Jan 29 15:12:05 informational %SYS-6-CLOCKUPDATE: System clock has been updated from 01:28:30 UTC Wed Mar 30 2011 to 15:12:05 UTC W...
Jan 31 20:30:29 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to down
Jan 31 20:30:31 notifications %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to up

To filter historical events, choose a severity filter or type filter:

- Debugging—Debug messages.
- Informational—Informational messages.
- Notifications—The switch is operating normally but has a significant condition.
- Warnings—The switch has a warning condition.
- Errors—The switch has an error condition.
- Critical—The switch has a critical condition.
- Alerts—The switch requires immediate action.
- Emergencies—The switch is unusable.

Click Clear Log to acknowledge that you have read the alerts. Clicking Clear Log does not resolve the issue.

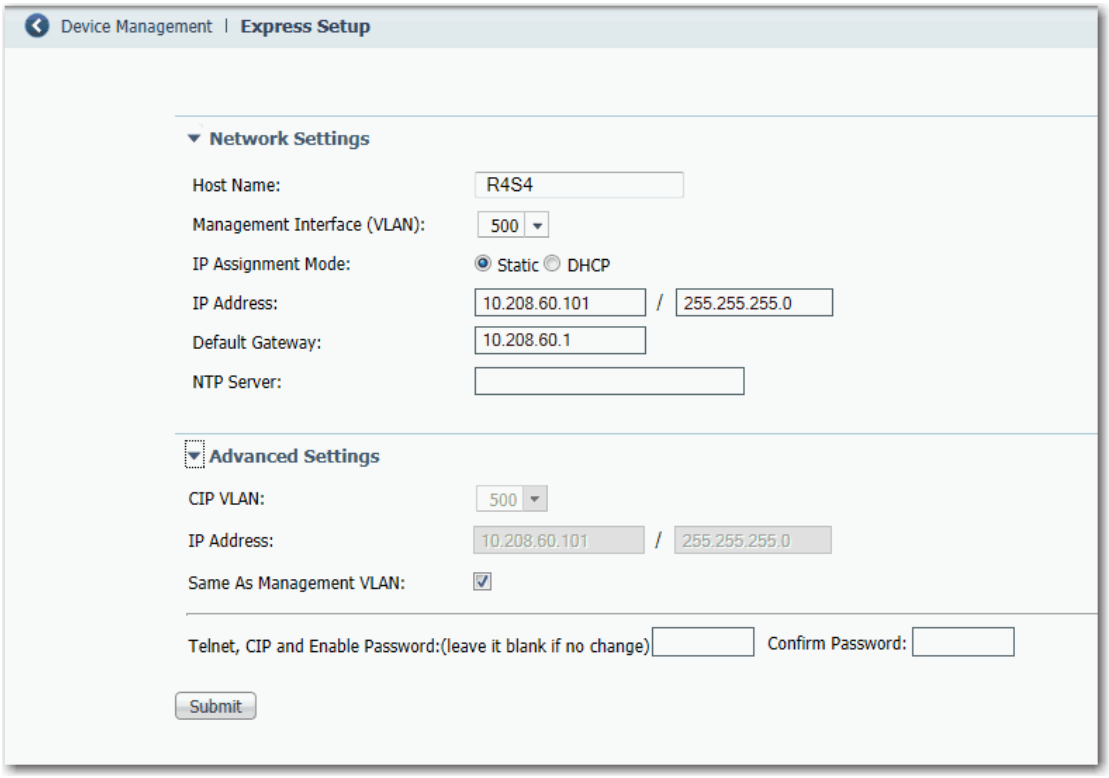
Table 22 - Syslog Fields

Field	Description
Time Stamp	The date and time the event occurred. Use the Express Setup window to connect the device to an NTP server. Time settings are lost if the switch loses power.
Severity Level	The type and severity of the event.
Description	The description of the problem, including the port on which the problem was detected.

Use Express Setup to Change Switch Settings

The network settings enable the switch to operate with its standard default settings and to be managed through the Device Manager Web interface. These settings were set during the initial setup. Change these settings if you want to move the switch to a different management VLAN or to a different network.

To update the switch IP information, from the Admin menu, choose Express Setup.

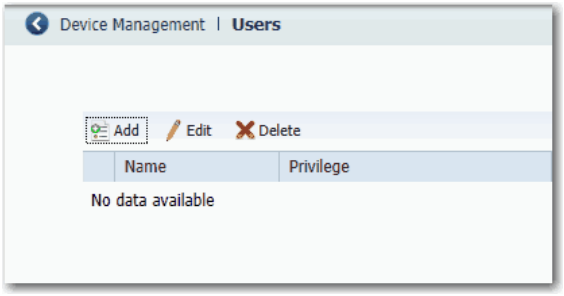


Field	Description
	Network Settings
Host Name	The name of the device.
Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch is managed. Choose an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1 . . . 1001. Be sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that must be limited to a specific group of users, such as the administrators of your network. It also provides secure administrative access to all devices in the network at all times.
IP Assignment Mode	The IP Assignment mode determines whether the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you click Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you click DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, be sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server automatically assigns to other devices. This prevents IP address conflicts between the switch and another device.

Field	Description
IP Address	The IP address and associated subnet mask are unique identifiers for the switch in a network: • The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. • The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same.
Default Gateway (optional)	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate with each other.
NTP Server	The IP address of the Network Time Protocol (NTP) server. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
Advanced Settings	
CIP VLAN	The VLAN on which Common Industrial Protocol (CIP) is enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on this device.
IP Address	The IP address and subnet mask for the CIP VLAN if the CIP VLAN is different from the management VLAN. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that the IP address that you assign to this device is not being used by another device in your network.
Same As Management VLAN	Indicates whether the settings for the CIP VLAN are the same as the management VLAN.
Telnet, CIP and Enable Password (optional)	The password used for Telnet and CIP security.
Confirm Password	The same password as above.

Manage Users

To add, modify, or delete users and user logon information for the switch, from the Admin menu, choose Users.



For each user, you can specify the information in the table below.

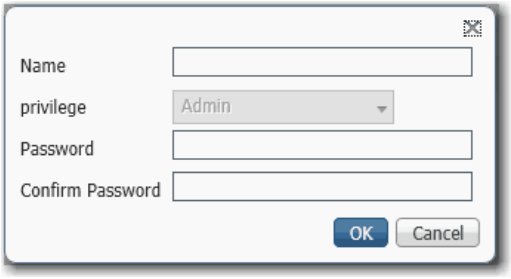


Table 23 - Add User Fields

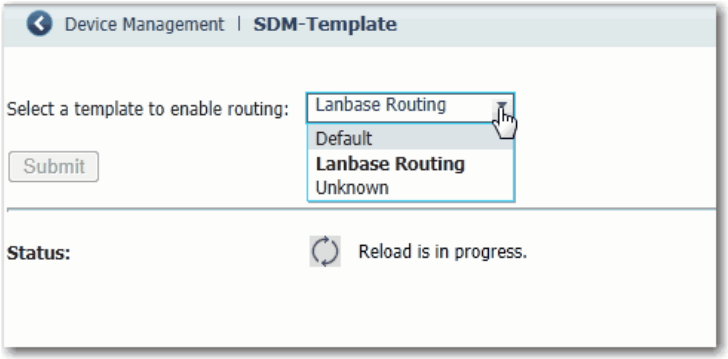
Field	Description
Name	The user name for this user.
Privilege	The level of access for this user. All users are assigned the Admin privilege and can change all parameters.
Password	The password that is required for access with this user name.
Confirm Password	The same password as above.

Reallocate Switch Memory for Routing

Switch Management Database (SDM) templates optimize how switch memory is allocated for specific features, such as routing. To enable routing, you must change the default SDM template to the Lanbase Routing template.

To apply an SDM template, follow these steps.

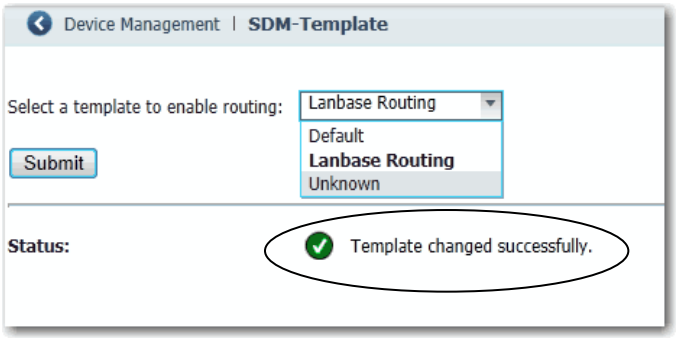
1. From the Admin menu, choose SDM-Template.
2. Choose a template from the pull-down menu:
   - Default—Gives balance to all Layer 2 functions
   - Lanbase Routing—Maximizes system resources for IPv4 unicast routing, which is required to enable routing
   - Unknown—User-configured from the CLI



3. Click Submit.
4. When a message appears prompting you to continue, click OK.

IMPORTANT The process of changing the template causes the switch to automatically restart.

A message appears once the process is complete.



5. To enable routing, proceed to Enable and Configure Routing on page 148.

Restart the Switch

Restarting or resetting the switch interrupts connectivity of your devices to the network.

To restart or reset the switch, from the Admin menu, choose Restart/Reset.

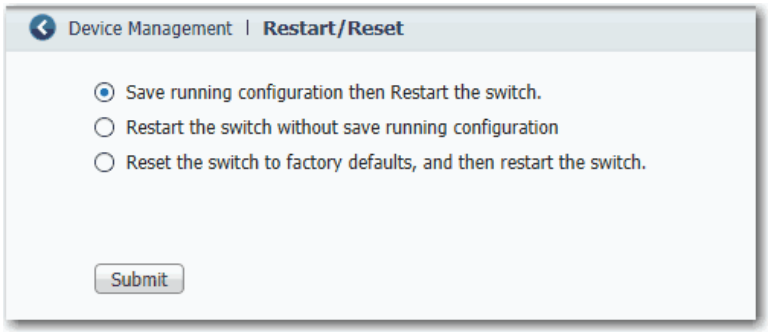

Device Management | Restart/Reset
Save running configuration then Restart the switch.
Restart the switch without save running configuration
Reset the switch to factory defaults, and then restart the switch.
Submit

Table 24 - Restart/Reset Fields

Field	Description
Save running configuration and then restart the switch.	Ensures that any changes in the running configuration are saved before the switch restarts.
Restart the switch without saving running configuration	Restarts the switch with its previously saved configuration settings.
Reset the switch to factory defaults, and then restart the switch	Resets the device to the factory-default settings, deleting the current configuration settings, and then restarts the device. You will lose connectivity with the device and need to initiate Express Setup to reconfigure the device.

Upgrade the Switch Firmware

You must have access to the Internet to download switch firmware from http://www.rockwellautomation.com to your computer or network drive.

To update the switch with the latest software changes and features, from the Admin menu, choose Software Update.

From the Device Manager Web interface, you can upgrade your switches one at a time.

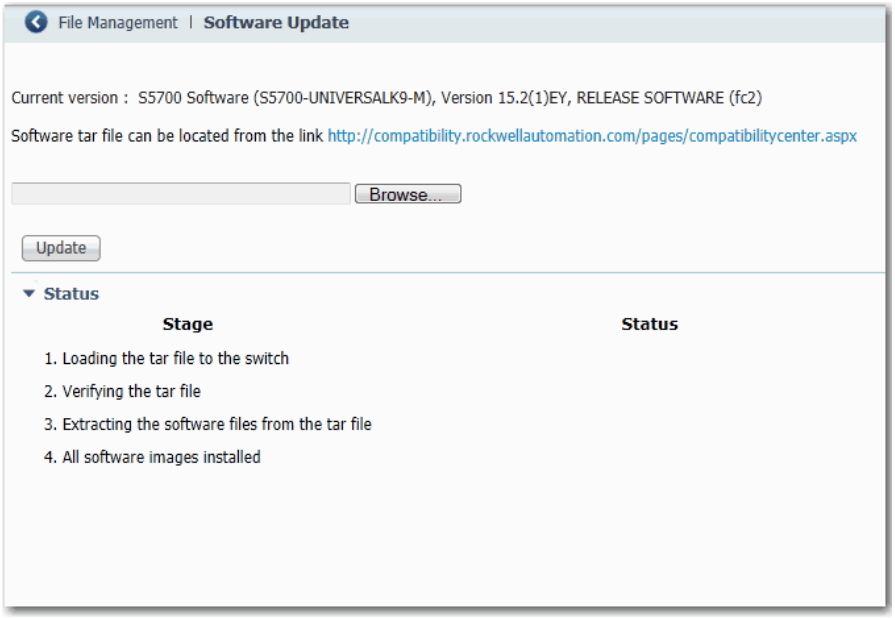
With firmware revision 2.001 or later, the firmware upgrade is installed to the running nonvolatile memory location:

- If you start the switch with the SD card inserted, the upgrade is installed on the SD card.
- If you start the switch from onboard memory without the SD card inserted, the upgrade is installed in the onboard flash memory.

IMPORTANT Wait for the upgrade process to complete. Do not use or close the browser session with the Device Manager Web interface active. Do not access the Device Manager Web interface from another browser session.

When the upgrade process completes, a success message appears, and the switch automatically restarts. It can take a few minutes for the switch to restart with the new firmware.

Verify that the latest firmware revision on the switch appears in the Software field in the Switch Information area of the dashboard.


File Management | Software Update
Current version : S5700 Software (S5700-UNIVERSALK9-M), Version 15.2(1)EY, RELEASE SOFTWARE (fc2)
Software tar file can be located from the link http://compatibility.rockwellautomation.com/pages/compatibilitycenter.aspx
Browse...
Update
Status
Stage
Status
1. Loading the tar file to the switch
2. Verifying the tar file
3. Extracting the software files from the tar file
4. All software images installed

See the Device Manager Web interface online help for additional guidelines and procedures.

Use the SD Card to Synchronize the Configuration or IOS Files

Use the Sync window to synchronize the SD card with the onboard memory. On the Manual Sync tab, you can view the following:

- Whether a card is present
- Card status
- If present, the source from which the switch was started

You can choose to synchronize the configuration or the software IOS from either the SD card to the onboard memory or from the onboard memory to SD card.

IMPORTANT You can overwrite your configuration if you synchronize in the wrong direction.

The Auto Sync tab lets you set up default options for how the Device Manager Web interface prompts the user after a configuration change or IOS update.

To display this window, from the Admin menu, choose Sync.

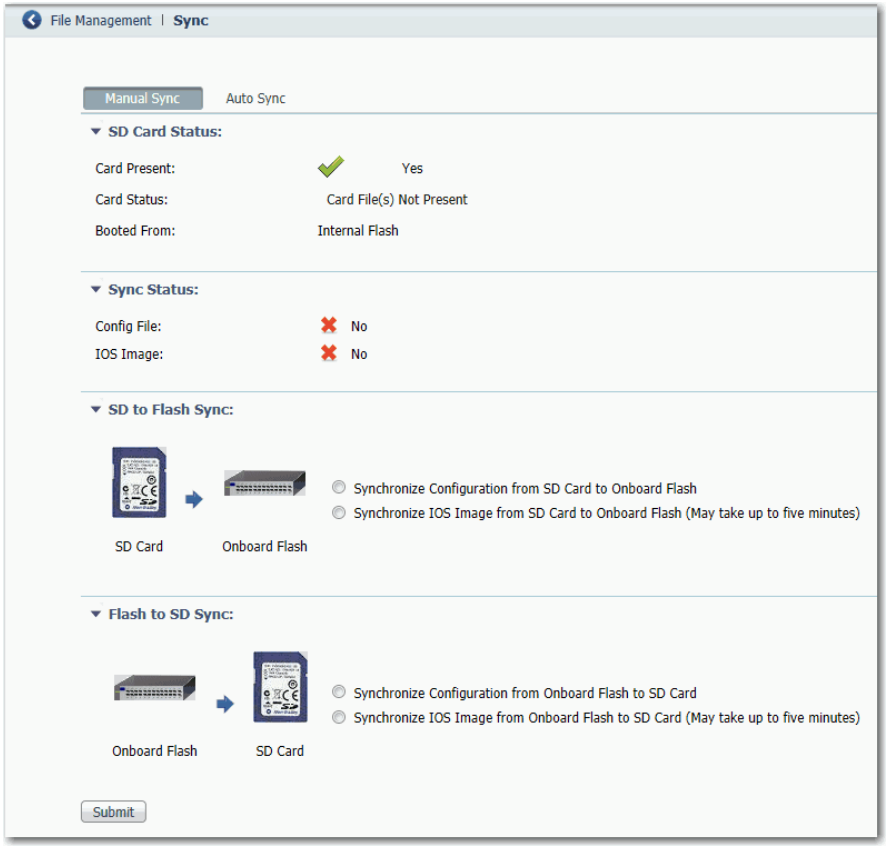


Table 25 - Manual Sync Tab Fields

Field	Description
SD Card Status	Indicates whether SD card is present, the card's status, and from where its configuration was started.
SD to Flash Sync	Choose from these options: • Synchronize configuration from SD card to onboard flash • Synchronize IOS image from SD card to onboard flash
Flash to SD Sync	Choose from these options: • Synchronize configuration from onboard flash to SD card • Synchronize IOS image from onboard flash to SD card

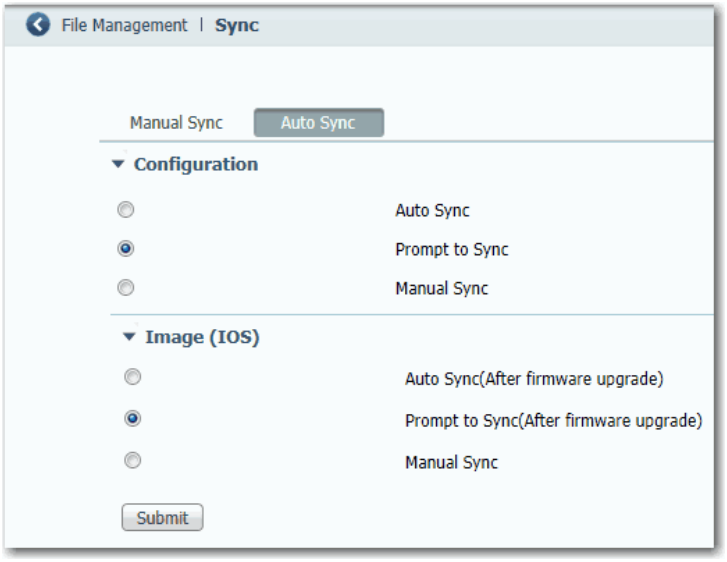


Table 26 - Auto Sync Tab Fields

Field	Description
Configuration	Auto Sync—Automatically synchronize the configuration when a configuration change is made in the Device Manager Web interface. This is the default configuration.
	Prompt to Sync—After a user has submitted a configuration change, the user is prompted with a message asking to confirm the synchronization.
	Manual Sync—No synchronization occurs on a configuration change unless the user performs a sync manually.
Image (IOS)	Auto Sync (After firmware upgrade)—Automatically sync the changed configuration when firmware is upgraded.
	Prompt to Sync (After upgrade)—After firmware is upgraded, the user is prompted with a message asking to confirm the configuration. This is the default configuration.
	Manual Sync—No synchronization occurs after firmware is upgraded unless the user performs a sync manually.

Upload and Download Configuration Files

To copy a configuration file from a file on another device, such as a PC, to the onboard memory, enter the directory name of the folder on the switch, browse to select the file, and click Upload.

To download a configuration file from the onboard memory to your computer, right-click the link and choose Save Link As.

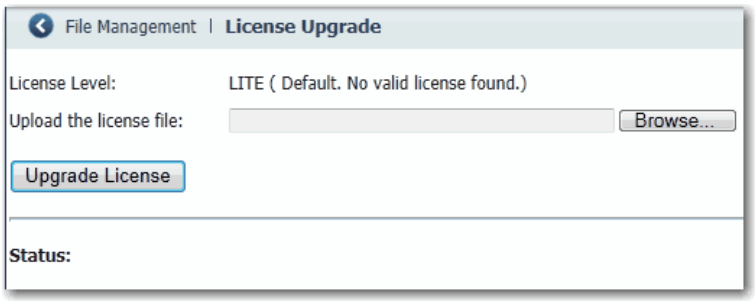
File Management | Load/Save
Booted From: Internal Flash
upload a file to device
Directory to be put flash:/
Browse...
Upload
Download configuration files from booting device(Please use save as, otherwise it may be a cached version. you may have to modify the file name)
config.text
vlan.dat
dmuser.txt

Upgrade License Files

After obtaining a license file, use the License Upgrade window to install it on the switch.

1. Click Browse to select the license file.
2. Click Upgrade License to begin the upgrade process.

   Messages appear to indicate the progress. Once the upgrade is complete, the switch restarts.



Manage the Switch via the Studio 5000 Environment

Topic	Page
EtherNet/IP CIP Interface	188
Add a Switch to the I/O Configuration Tree	191
Configure General Properties	192
Connection Properties	195
Module Information	196
Switch Configuration Properties	197
Switch Status	199
Port Configuration	200
Power over Ethernet (PoE)	201
Smartports and VLANs	203
Port Thresholds	205
Port Security	206
Port Status	207
Port Diagnostics	208
Cable Diagnostics	209
DHCP Pool Display	210
DHCP Address Assignment	212
Time Sync Configuration	213
NAT Configuration	215
NAT Diagnostics	229
SD Flash Sync	233
Save and Restore the Switch Configuration	234

After you complete Express Setup, you can manage the switch by using the Studio 5000 Logix Designer™ application in the Studio 5000 Automation Engineering & Design Environment.

EtherNet/IP CIP Interface

Stratix 5700 switches contain an EtherNet/IP network interface. The EtherNet/IP network is an industrial automation network specification maintained by the Open DeviceNet Vendor Association (ODVA). It uses the Common Industrial Protocol (CIP) for its application layer and TCP/UDP/IP for its transport and network layers. This interface is accessible via any of the switch's Ethernet ports by using the IP address of the switch.

CIP Network Connections

CIP is an object-oriented connection-based protocol that supports two basic types of messaging: explicit and implicit (I/O) connections. A maximum of 32 connections is available. Both connection types must use the switch password before any switch parameters can be written. The password is the same one you enter during Express Setup.

Table 27 - CIP Network Connections

Connection	Description
Explicit messaging	Explicit messaging connections provide generic, multi-purpose communication paths between two devices. These connections are often referred to as messaging connections. Explicit messages provide request/response-oriented network communication. Each request is typically directed at a different data item. Explicit messages can be used for configuring, monitoring, and troubleshooting the switch. The Explicit Messaging interface is used by the Logix Designer application.
I/O (implicit messaging)	I/O connections provide dedicated, special purpose communication paths between a producing application and one or more consuming applications. The application-specific I/O data that moves through these connections is typically a fixed, cyclical structure. The switch supports two I/O connection choices. • Input Only • Exclusive Owner Both connections are cyclic and adjustable from 300...5000 ms. The Input Only connection contains a data structure with status information on the switch in general and specific status on each of the ports. This connection is multicast and can be shared by multiple controllers (connection originators). The Exclusive Owner connection uses the same Input data structure as the Input Only connection, but adds an Output data structure. The Output data contains a bit for each port that lets you enable or disable each port separately. While the Input data on this connection can be shared (via multicast) by multiple controllers, only one controller can own the Output data. If a second controller attempts to open this connection, the connection is rejected.

IMPORTANT Because the output data is sent cyclically by the controller, it overrides any other attempt to enable or disable a port from other software tools or visualization stations.

RSLinx Software and Network Who Support

The EtherNet/IP network interface also supports the List Identity command used by CIP-based network tools, such as the RSLinx® software RSWho function. RSWho enables you to locate and identify your switch on the network by using the electronic data sheet (EDS) files.

To access the RSWho function, from the RSLinx software toolbar, choose Communications > RSWho.

IMPORTANT After using the RSWho function, if you access the switch and view the Ethernet link counters, you see the counts for only the first port (Port Gi1/1).

Electronic Data Sheet (EDS) Files

Electronic Data Sheet (EDS) files are simple text files used by network configuration tools, such as RSNetWorx™ for EtherNet/IP software, to help you identify products and easily commission them on a network. EDS files contain details about the readable and configurable parameters of the device. They also provide information about the I/O connections the device supports and the content of the associated data structures.

If you are using the switch in a system that does not have a Rockwell Automation Logix-based controller to monitor or control your switch, you cannot use the AOP supplied with Logix controllers. You must use information from the EDS files to set up the I/O connection.

The OPC Server contained in RSLinx Classic software also uses EDS files to provide you with a list of parameters when adding items (OPC Tags) to a Topic (the switch).

EDS files for the Stratix 5700 switches are included with the following software packages:

- RSLinx software, version 2.54 or later
- RSLogix 5000 software, version 16 or later, or the Logix Designer application, version 21.00.00 or later
- RSNetWorx for EtherNet/IP software, version 9.0 or later

You can also obtain the EDS files in either of these two ways:

- From http://www.rockwellautomation.com/resources/eds/.

  TIP To locate a specific EDS file, do the following:

  - Choose EtherNet/IP from the Network type field.
  - Enter Stratix 5700 in the Keyword field.
  - Leave the other fields with their default entries.

- From the switch by using the RSLinx EDS Hardware Installation Tool.

To upload the EDS files directly from the switch over the network, follow these steps.

1. From the Start menu, choose Programs > Rockwell Software > RSLinx >Tools > EDS Hardware Installation Tool.
2. Click Add to launch the EDS Wizard and add the selected hardware description and associated files.

Data Accessible With CIP

The CIP interface lets you access the following information:

- Input data via I/O connection

  –Link status per port: not connected, connected
  –Unauthorized device per port: OK, not OK
  –Unicast threshold exceeded per port: OK, exceeded
  –Multicast threshold exceeded on each port: OK, exceeded
  –Broadcast threshold exceeded on each port: OK, exceeded
  –Port bandwidth utilization per port: value in %
  –Alarm relay major: OK, tripped
  –Multicast groups active: quantity

- Output data via I/O connection

  –Port disable per port: enabled, disabled

- Other status data

  – Switch internal temperature: degrees Centigrade
  – Power supply A present: yes, no
  – Power supply B present: yes, no
  – Identity information: vendor ID, device type, product code, product name, revision, serial number
  – IOS release version
  – Switch uptime since last restart
  – Management CPU utilization: in percentage
  – CIP connection counters: open/close requests, open/close rejects, timeouts
  – Port alarm status per port: OK, not forwarding, not operating, excessive FCS errors
  – Port fault status per port: Error Disable, SFP error, native VLAN mismatch, MAC address flap condition, security violation
  – Port diagnostic counters per port: Ethernet interface counters (10), Ethernet media counters (12)

- Configuration data (requires password)
  - IP address method: DHCP, static
  - IP address, subnet mask, default gateway (all if static)
  - Host name
  - Contact name
  - Geographic location
  - Port configuration per port: enable/disable, autonegotiate, forced speed/duplex
  - Authorized MAC ID per port
  - Unicast rate limiting threshold per port: in packets per second, bits per second, or percentage
  - Multicast rate limiting threshold: in packets per second, bits per sec, or percentage
  - Broadcast rate limiting threshold: in packets per second, bits per sec, or percentage
- Smartport assignment per port: role and VLAN
- Save and restore of switch configuration (via File Obj)

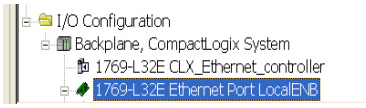
Add a Switch to the I/O Configuration Tree

To add the switch to the controller's I/O tree, follow these steps.

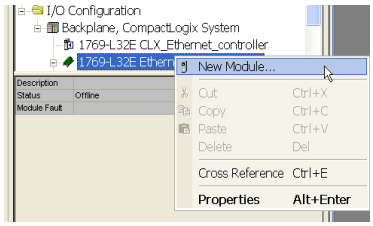
IMPORTANT These steps are required before you can go online to configure and monitor the switch.

1. Open the project file for the controller that monitors the switch.
2. Select the Ethernet module through which the controller communicates with the switch.

   In this example, the switch communicates through a 1769-L32E CompactLogix EtherNet/IP controller.



3. Right-click the Ethernet port you created and choose New Module.



4. Click Communications.

5. Click the + sign and scroll down until you see the switch you want to configure.

   If you do not see the switch on the list, you can obtain the AOP from the Rockwell Automation support website.

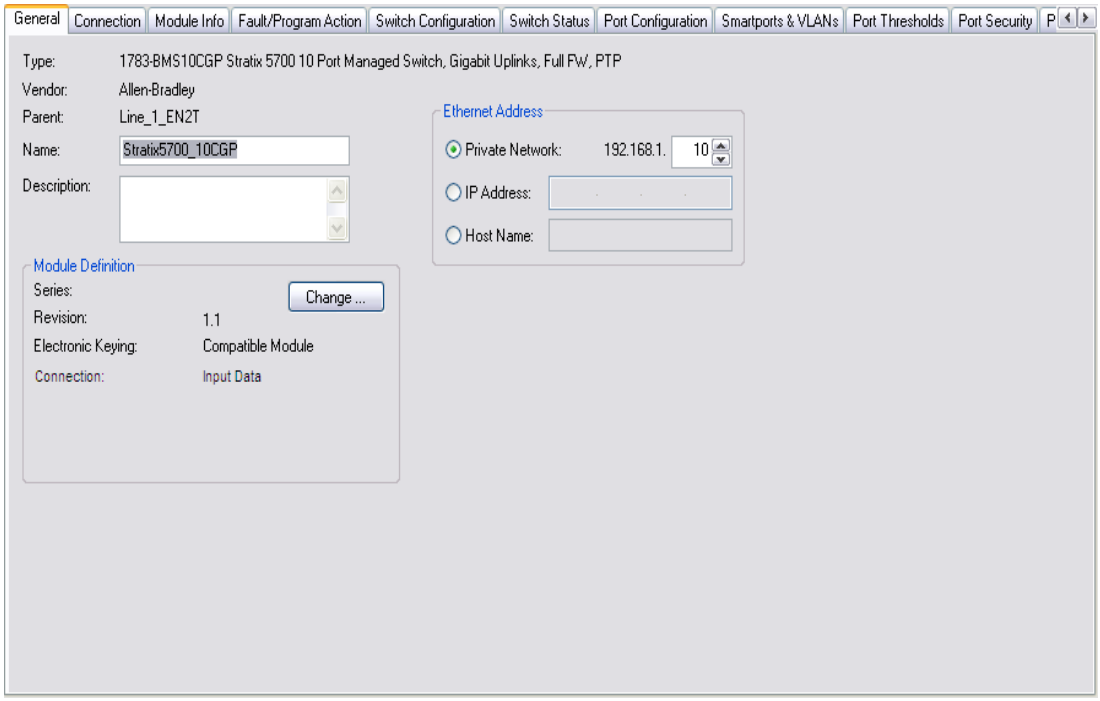
   a. Go to http://www.rockwellautomation.com/support/.

   b. Click Downloads/RSLogix 5000 I/O Modules Add-on Profiles.

   c. Choose the 1783-Stratix 5700 Managed Switches Add-on Profile.

6. Click OK to display the Module Properties dialog box.

Configure General Properties



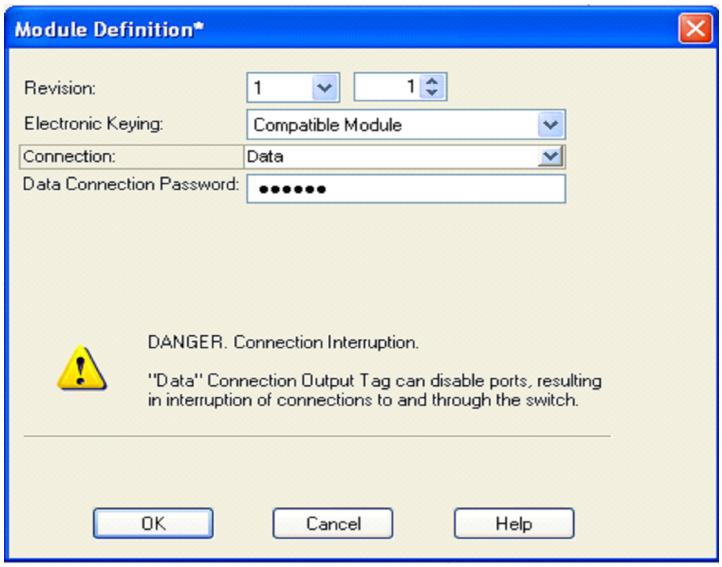
To configure general properties, follow these steps.

1. From the Module Properties dialog box, complete the fields described below.

Field	Description
Name	A name you choose for the switch.
Description	A description that helps you remember something important about the switch.
Ethernet Address	Choose one of the following: • Private Network—The private network on which the switch resides. • IP Address—The IP address you entered when you performed the Express Setup. The controller uses the IP address to communicate. • Host Name—The host name provided on initial configuration when you performed the Express Setup.The host name requires that you have a DNS server configured on the network for the controller's Ethernet interface module. **IMPORTANT:** Be sure that the IP address and host name are the same as those provided when you performed Express Setup.

2. Click OK.
3. Go online with the switch by choosing Communications > Go online.
4. Double-click the switch to view the Module Properties dialog box.
5. Click Change.

6. Complete the fields on the Module Definition dialog box.



Field	Description
Revision	The major and minor revision of the switch: • Major revision: a number from 1…128 • Minor revision: a number from 1…255
Electronic Keying	• Compatible Module (default) • Exact Match • Disable Keying
Connection	• Input Data (default): Enables only the input data connection • Data: Enables input and output data connection **ATTENTION:** This selection enables output tags, which can disable ports and interrupt connections to and through the switch. You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied. The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using the Device Manager Web interface or the CLI, the port setting can be overridden by the output bits from the controller on the next cyclic update of the I/O connection. The output bits always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.
Data Connection Password	Enter the password for accessing the switch. Required only for Data connection.

Connection Properties

You can define connection properties for the switch on the Connection tab.

Table 28 - Connection Tab Fields

Field	Description
Requested Packet Interval (RPI)	Enter a value between 300…5000.
Inhibit Module	Check to disable communication between the controller and the switch. Clear the checkbox to restore communication.
Major Fault on Controller If Connection Fails While in Run mode	Check to have the controller create a major fault if connection fails in Run mode.
Use Unicast Connections over EtherNet/IP	Check to use Unicast connections with the EtherNet/IP network.
Module Fault	Displays the fault code returned from the controller (related to the switch you are configuring), and the text detailing the module fault has occurred.

Module Information

You can monitor and reset the switch from the Module Info tab.

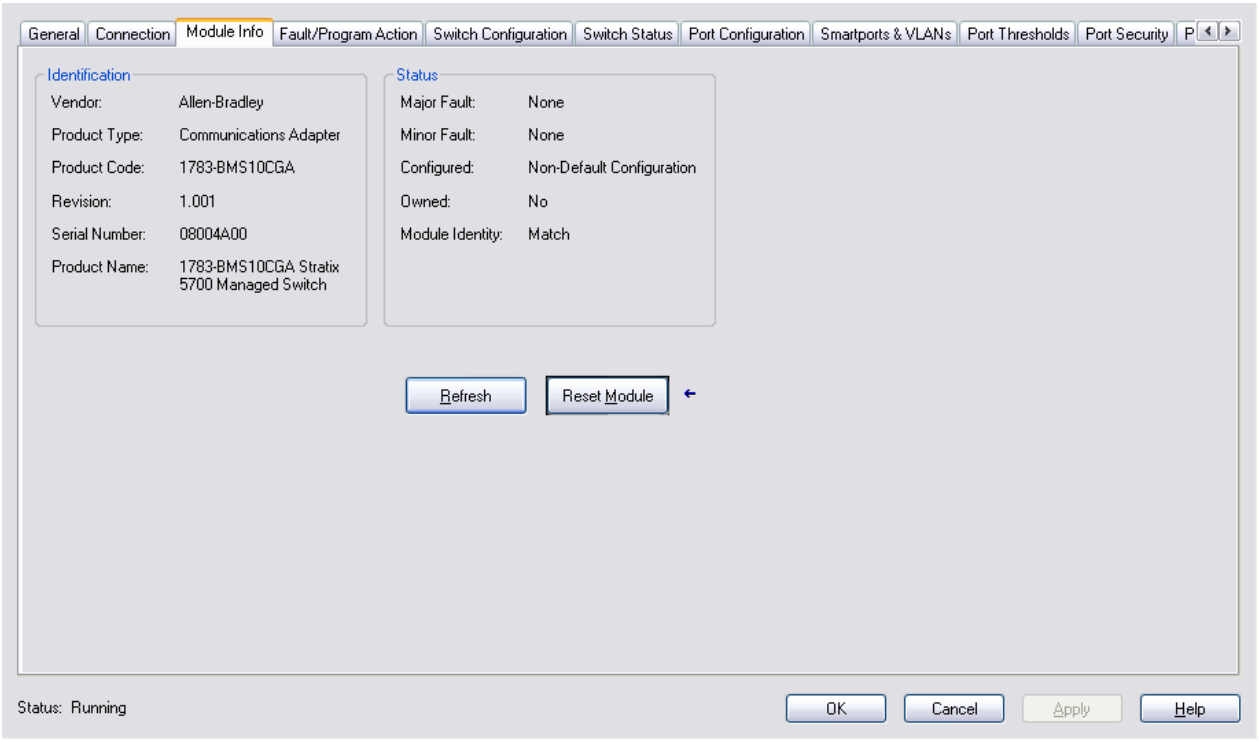


Table 29 - Module Info Tab Fields

Field	Description
Identification	Displays the following information about the switch: • Vendor • Product type • Product code • Revision • Serial number • Product name
Status	Displays the status of the following: • Major/minor fault status: – None – Recoverable – Non-recoverable • Configuration: – Non-default configuration – Default configuration • Owned. Indicates whether there is an I/O connection: – Yes – No • Module identity: – Match. Agrees with what is specified on the General tab. In order for the Match condition to exist, the vendor, product type, product code, and major revision must agree. – Mismatch. Does not agree with what is specified on the General tab. The Module Identify field does not take into account the Electronic Keying or Minor Revision selections for the switch that were specified on the General tab.
Refresh	Click to refresh the tab with new data from the module.
Reset Module	Click to perform a switch reset (power cycle) with the current configuration file. The Password Confirmation dialog box can appear. **ATTENTION**: Resetting a module causes all connections to or through the module to be closed. This can result in loss of control.

Switch Configuration Properties

You can configure IP settings and administrative parameters from the Switch Configuration tab. You must be online to perform these configurations. In Offline mode nothing is displayed on this tab.

The IP address can be manually assigned (static) or it can be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you choose Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.

- Static—Manually enter the IP address, subnet mask, and gateway.
- DHCP—The switch automatically obtains an IP address, default gateway, and subnet mask from the DHCP server. As long as the switch is not restarted, it continues to use the assigned IP information.

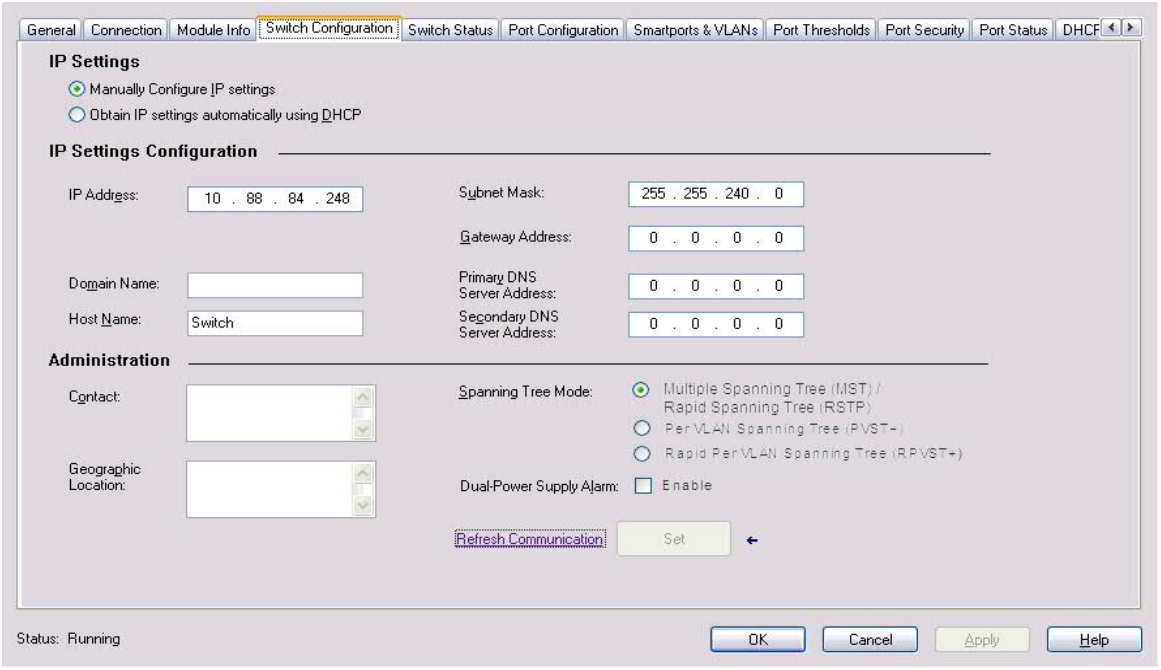


Table 30 - Switch Configuration Tab Fields

Field	Description
IP Address	This value must match the IP address on the General tab. If you reconfigure your switch with a different IP address, you can lose communication with the switch when you click Set. To correct this problem, you must go back to the Express Setup and General tab, set the new IP address, and download to the controller.
Subnet Mask	Enter the appropriate subnet mask for the switch. The subnet mask is a 32-bit number. Set each octet between 0…255. The default is 255.255.255.0.
Gateway Address	A gateway is a router or other network device through which the switch communicates with devices on other networks or subnetworks. The gateway IP address must be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. **IMPORTANT:** Communication is disrupted when you change the gateway (IP) address.
Primary DNS Server Address	Enter the IP address of the primary Domain Name Server (DNS). Set each octet between 0…255. The first octet cannot be 127 or a number greater than 223.
Secondary DNS Server Address	Enter the IP address of the secondary Domain Name Server (DNS). Set each octet between 0…255. The first octet cannot be 127 or a number greater than 223.
Domain Name	Enter the name of the domain in which the module resides. The domain name consists of a sequence of name labels separated by periods, such as example.com. The domain name has a 48-character limit and is restricted to ASCII letters a…z, digits 0…9, and periods and hyphens.
Host Name	(Optional). Enter a name to help identify the switch when monitoring or troubleshooting a problem. The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Contact	(Optional). Enter contact information for the switch, up to 200 characters. The contact information can include alphanumeric and special characters (dash and comma) and a carriage return.
Geographic Location	(Optional). Enter a geographic location of the switch, up to 200 characters. The geographic location can include alphanumeric and special characters (dash and comma) and a carriage return.
Spanning Tree Mode	Choose one of the following: • RSTP/MST • PVST+ • RPVST+ RSTP/MST is the default.
Dual-Power Supply Alarm	Check the checkbox to enable the feature. The feature is disabled by default.
Refresh	Click to refresh the tab with new data from the switch.
Set	Click to save the settings to the switch and the SD card, if installed. Once the password has been entered correctly, changes can be made within 10 minutes without the Enter Password dialog box prompting you for a password.

Switch Status

From the Switch Status tab, you can view various status parameters for the switch.

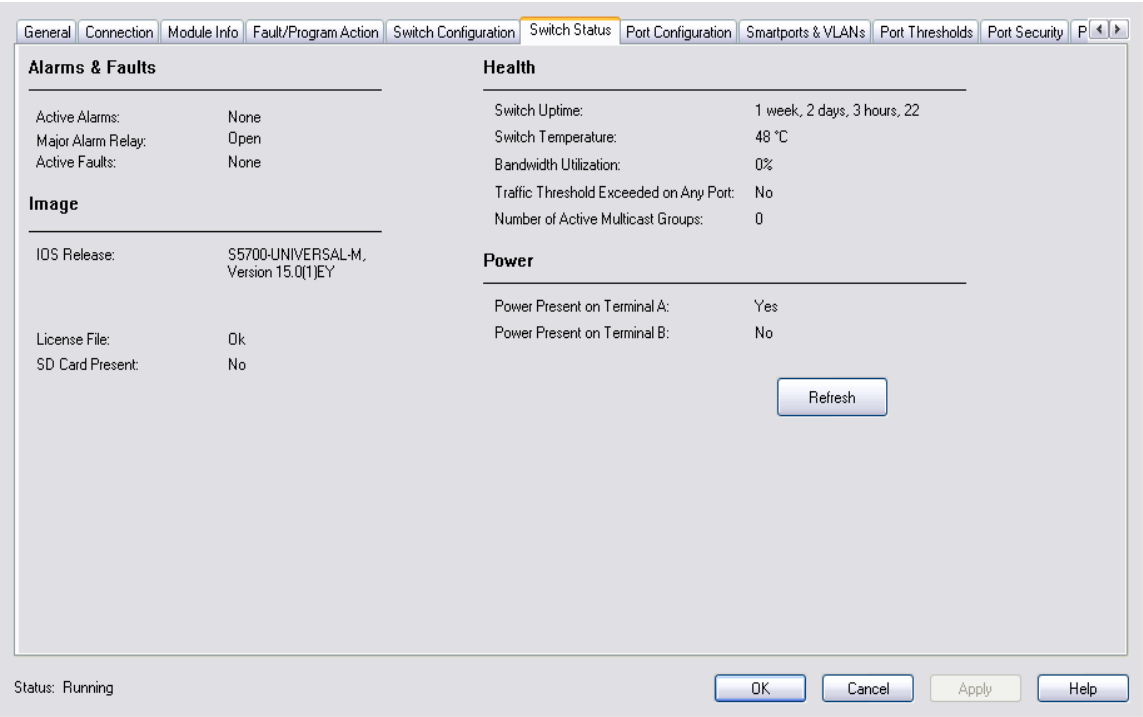


Table 31 - Switch Status Tab Fields

Field	Description
Active Alarms	Displays one of these values: • None • Port alarm • Dual Mode Power Supply alarm • Primary Temperature alarm
Major Alarm Relay	Displays one of these values: • Open • Closed
Active Faults	Displays one of these values: • None • Port fault • Hardware fault If the port and hardware faults are active, the Hardware fault status appears.
Traffic Threshold Exceeded on Any Port	Displays a yes or no value indicating whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port. To view the status of the active ports, click the Port Status tab. To view the threshold values, click the Advanced - Port Threshold tab.
Switch Uptime	Displays the days, hours, and minutes that the switch has been functioning since the last restart.
Switch Temperature	Displays the current internal temperature (in degree Celsius) of the switch.
Bandwidth Utilization	Displays the total percentage of the switch bandwidth being used.
Power Present on Terminal A	Displays a yes or no value indicating whether power is present on Terminal A.
Power Present on Terminal B	Displays a yes or no value indicating whether power is present on Terminal B.
Number of Active Multicast Groups	Displays the number of active multicast groups.
IOS Release	Displays the current version of the switch operating system.

Port Configuration

Port configuration settings determine how data is received and sent between the switch and the attached device.

You must be online to configure the port features. Most of the information on this tab is not displayed if you are offline.

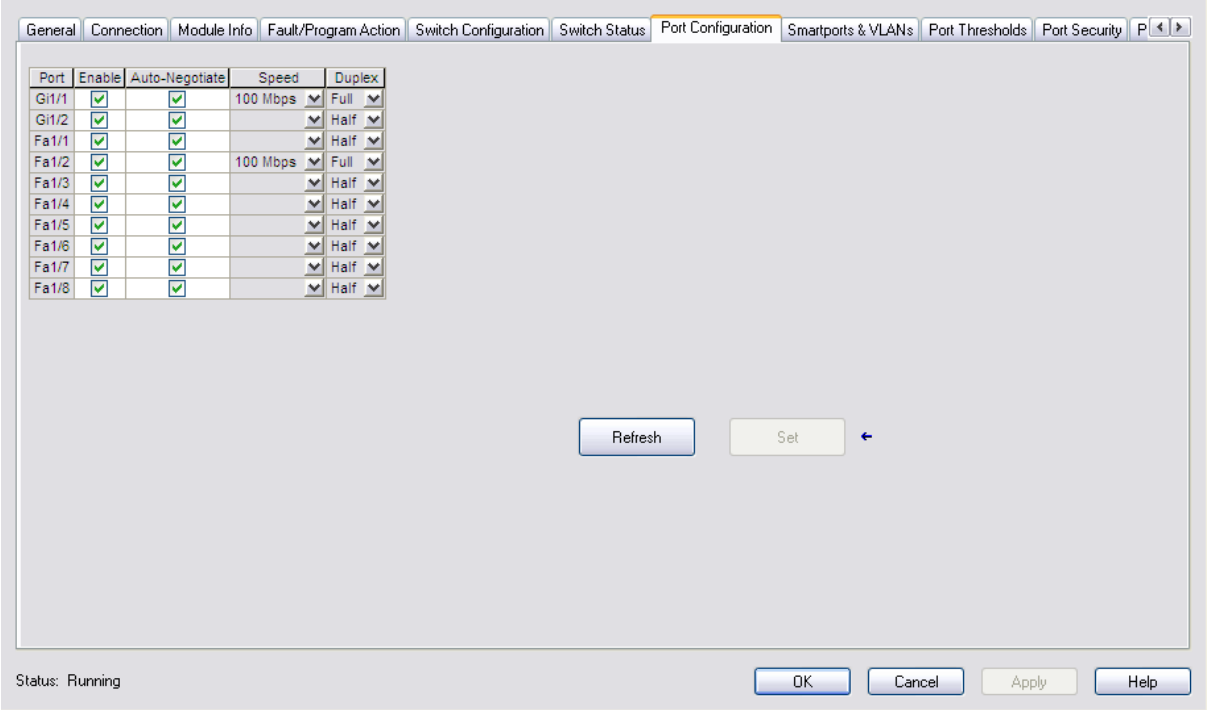


Table 32 - Port Configuration Tab Fields

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Enable	Check the checkbox to enable the port. Clear the checkbox to manually disable (shut down) the port. We recommend that you disable the port if the port is not in use and is not attached to a device. You can troubleshoot a suspected unauthorized connection by manually disabling the port.
Auto-negotiate	Check the checkbox if you want the port and end-device to auto-negotiate the link speed and Duplex mode. Clear the checkbox to manually specify the desired port speed and Duplex mode. We recommend that you use the default (auto-negotiate) so that the speed and duplex settings on the switch port automatically match the setting on the connected device. Change the switch port speed and duplex if the connected device requires a specific speed and duplex. If you set the speed and duplex for the switch port, the connected device must also be configured for the exact same speed and duplex, and not set to auto-negotiate, otherwise a speed/duplex mismatch occurs. Fiber optic interfaces do not support auto-negotiation.
Speed	Choose the operating speed of the port. Gigabit (Gi): • 10 Mbps • 100 Mbps • 1 Gbps Fast Ethernet (Fa): • 10 Mbps • 100 Mbps
Duplex	Choose one of these Duplex modes: • Half-duplex—Both devices cannot send data at the same time. Half-duplex is not available when speed is set to 1 Gbps. • Full-duplex—Both devices can send data at the same time.

Power over Ethernet (PoE)

PoE and PoE+ features are supported on switches with PoE ports when a correct power supply is connected to the switch. For power supply requirements, see page 44.

You can do the following from the PoE window:

- Limit the total power supported.
- Configure mode and power settings for individual ports.

For most applications, the default configuration (Auto mode) is sufficient and no further configuration is required. However, you can customize the settings to meet your needs. For example, to give a PoE port higher power priority, set the mode to Static and allocate the power to be used. As another example, to disallow high-power devices on a port, set the mode to Auto and specify a maximum power limit.

IMPORTANT When you make PoE configuration changes to a port, the port drops power. Whether the port powers up again depends on the new configuration, the state of the other PoE ports, and the state of the power budget.

For example, if port 1 is in Auto mode and the On state, and you configure it for Static mode, the switch removes power from port 1, detects the powered device, and repowers the port.

If port 1 is in Auto mode and the On state and you configure it with a maximum wattage of 10 W, the switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

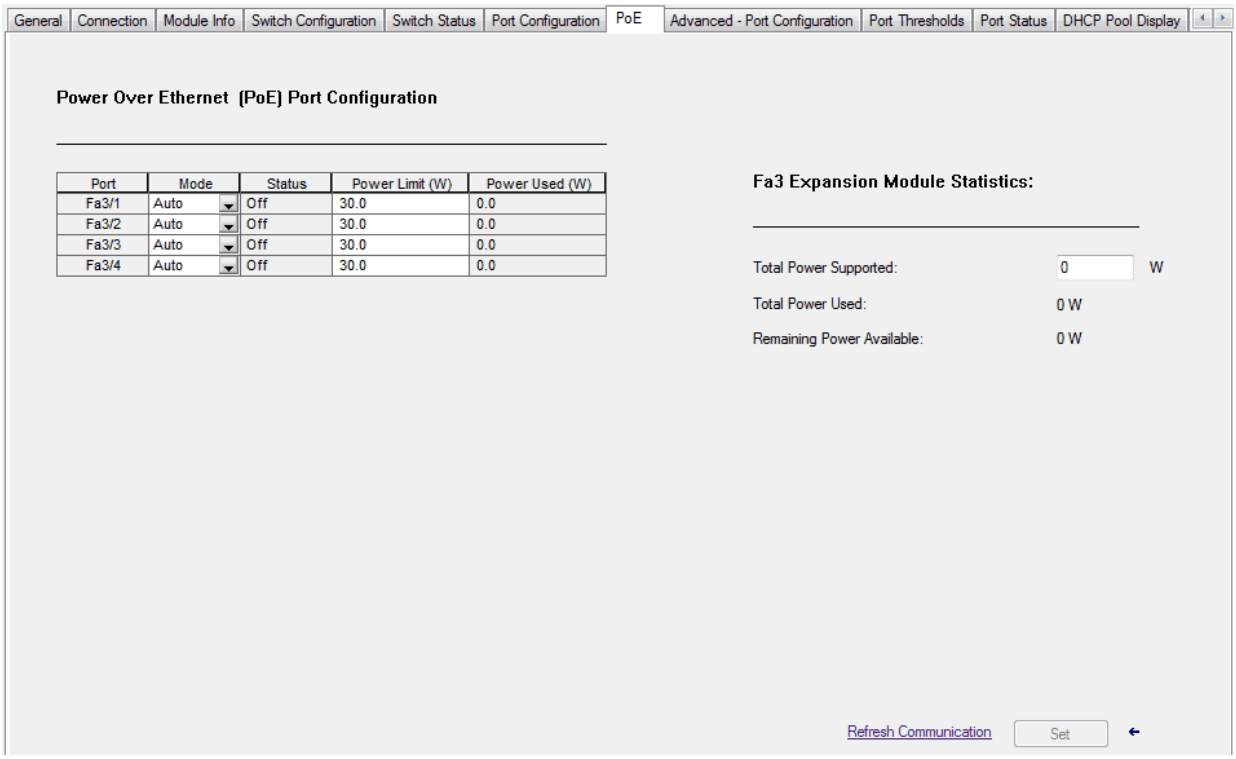


Table 33 - PoE Tab Fields

Field	Description
Port	Displays the port number.
Mode	Displays the Power Management mode of the port: • Auto—Enables the detection of powered devices and automatically allocates power to the PoE port if a device is connected. This setting is selected by default. To limit the power used by this port, adjust the value Power Limit field. • Static—Reserves power for this port even when no device is connected to make sure that power is provided upon device detection. You can also choose Static mode to prioritize a port. The switch allocates power to Static mode ports before it allocates power to Auto mode ports. • Off—PoE is disabled. For more information, see Power Management Modes on page 87.
Status	Displays the current status of the port: • 0—The status is unknown. • 1—PoE is enabled. Power is supplied to the port with no errors. • 2—PoE is not enabled. Power is not supplied to the port. • 3—PoE is enabled, but the switch denied power to the port. • 4—PoE is enabled, but a system fault occurred while power was supplied to the port. • 5—PoE is enabled, but the port overdrew power.
Power Limit (W)	Displays the maximum amount of power available to the port: PoE ports: 4…15.4 W PoE+ ports: 4…30 W If the port is in Auto mode, you can enter a value. The default value is 15.4 W.
Power Used (W)	Displays the amount of power currently in use by the port. If the port is in Auto mode, the default value is 15.4 W. If the port is in Static mode, you can enter a value to reserve power for the port.

Table 33 - PoE Tab Fields (continued)

Field	Description
Total Power Supported	To limit the total PoE power budget, type an appropriate value based on the power source: • A 48V power source supports a maximum of 65 W. • A 54V power source supports a maximum of 130 W. When you save this setting, it changes the total PoE power budget and resets the powered devices to meet the new budget. **IMPORTANT:** A mismatch between the total power supported and the power supply can cause damage to the switch. Take care not to oversubscribe the power supply: • If you intend to connect the switch to a power supply that allows more wattage than configured, first change the power supply and then specify the total power supported. • If you intend to connect the switch to a power supply that allows less wattage than configured, first change the total power supported to an appropriate value and then change the power supply.
Total Power Used	Displays the amount of power in watts the module is currently using.
Remaining Power Available	Displays the amount of unused power in watts available to the module.

Smartports and VLANs

From the Smartports & VLANs tab, you can assign Smartport roles and VLANs to ports on the switch. You can also create, edit, and delete VLANs. You must be online to configure these port features. Most of the information on this tab is not displayed if you are offline.

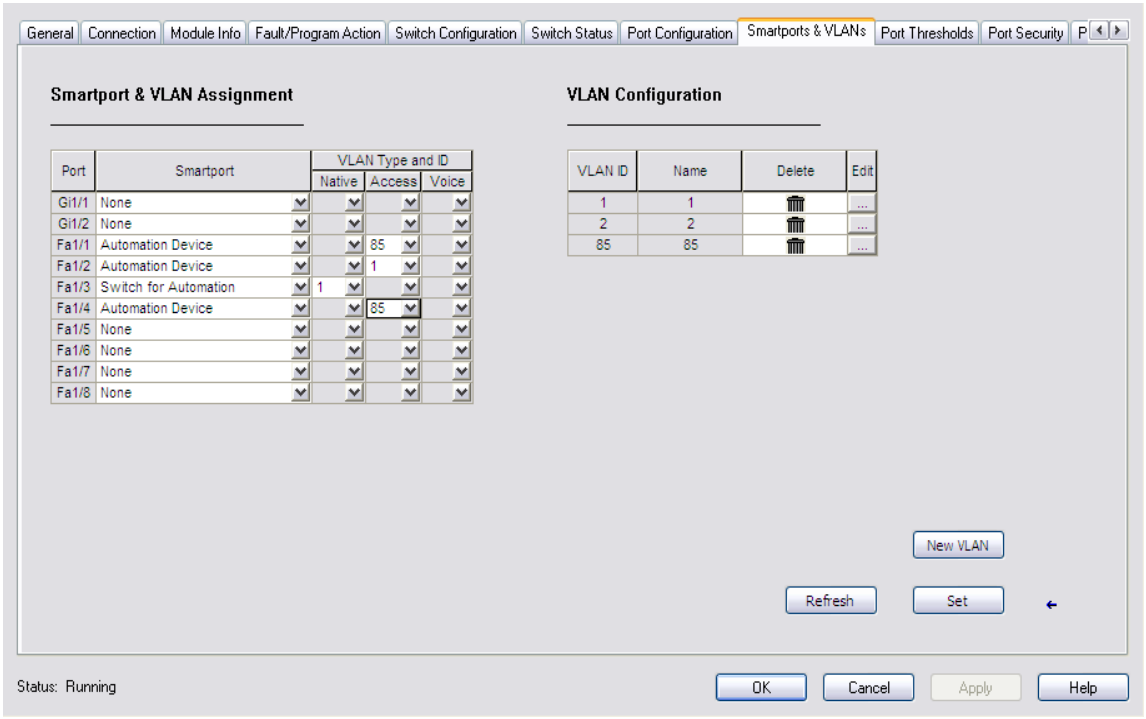


Table 34 - Smartports and VLANs Tab Fields

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Smartport	Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and provide security, transmission quality, and reliability to traffic from the switch ports. These configurations also prevent many problems caused by port misconfigurations. The port roles are based on the type of device that is connected to the switch port. Make sure you decide which port is connected to which type of device before you choose a Smartport role. Choose one of these Smartport roles to apply to the connected port: • Automation Device—Apply this role to ports to be connected to EtherNet/IP devices. It can be used for industrial automation devices, such as logic controllers and I/O. – Port is set to Access mode. – Port security supports only one MAC ID. – Optimize queue management for CIP traffic. • Desktop for Automation—Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts. Do not apply this role to ports to be connected to switches, routers, or access points. – Port is set to Access mode. – Portfast enabled. – Port security supports only one MAC ID. • Switch for Automation—Apply this role to ports to be connected to other switches. – Port is set to Trunk mode. – Portfast enabled. • Router for Automation—Apply this role to routers or ports to be connected to Layer 3 switches with routing services enabled. • Phone for Automation—Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer have network access through the port. This role prioritizes voice traffic over general data traffic to provide clear voice reception on the IP phones. – Port is set to Trunk mode. – Port security supports three MAC IDs to this port. • Wireless For Automation—Apply this role to ports to be connected to wireless access points. The access point can provide network access to up to 30 mobile (wireless) users. • Port Mirroring—Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 113. • None—Apply this role to ports if you do not want a specialized Smartport role on the port. This role can be used on connections to any device, including devices in the roles described above. • Custom—Create these roles for your application. You can set the type of VLAN you implement, if any. – Enter the name for the macro. Macro names are case sensitive. The string can be up to 31 alphanumeric characters. The string cannot contain a ?, a space, or a tab. – Choose a macro icon (CS1 to CS10).
VLAN Configuration	Displays the VLAN ID and name: • VLAN ID—The unique identifier (in a range of 2 . . . 4094; 1002 . . . 1005 reserved) for a VLAN you create by clicking Add New VLAN. VLAN ID 1 is the default. • Name—The unique name for the VLAN (20 characters maximum) you create by clicking Add New VLAN.

Port Thresholds

You can configure threshold limits for broadcast, unicast, and multicast traffic for each active port on the Port Thresholds tab. This feature is available only with Full firmware. The number of packets being sent is compared against the threshold value. These limits help to prevent a single device from sending too much traffic. For more information about this feature, see Port Thresholds on page 95.

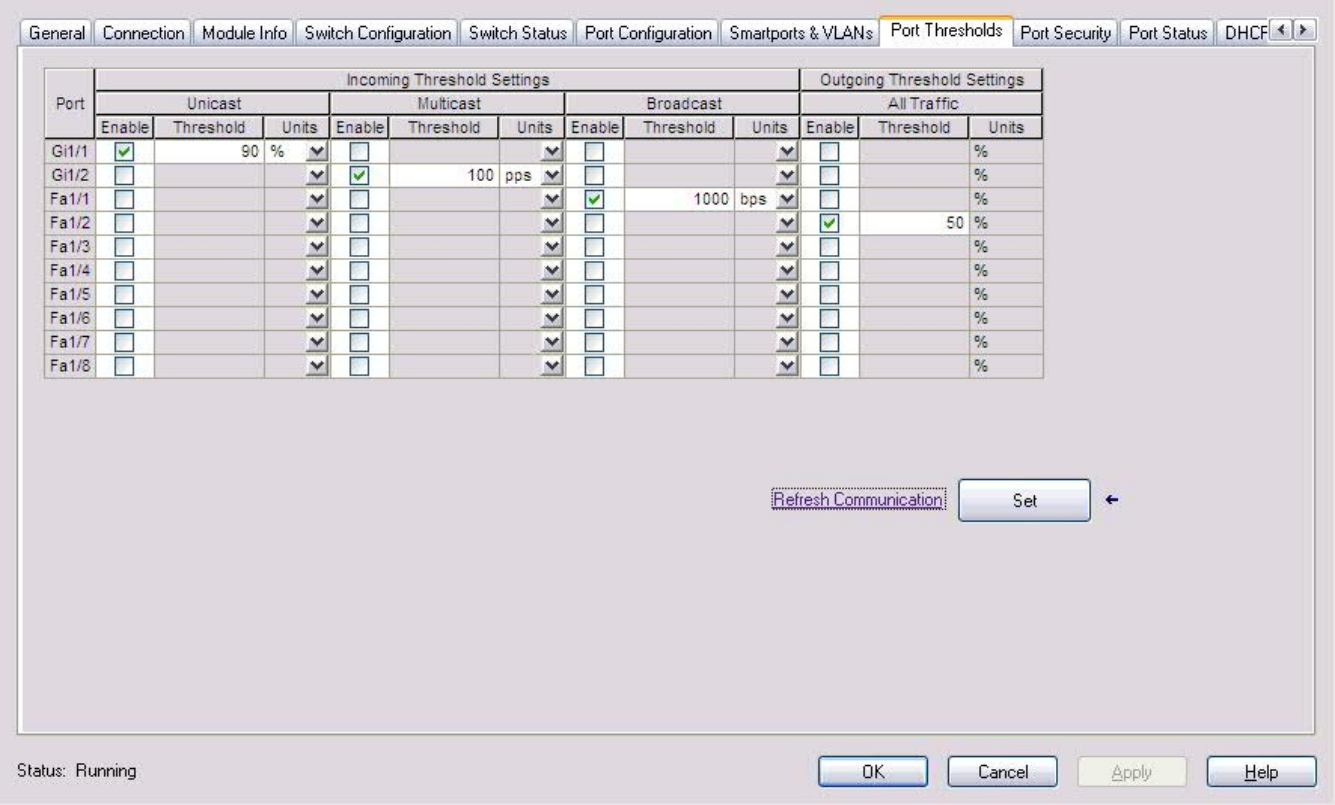


Table 35 - Port Threshold Tab Fields

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Incoming Threshold Settings	Enable incoming thresholds and set the threshold values for the unicast, multicast, and broadcast traffic for each port. Valid values for units: • Packets per second (pps) • Percentage of total bandwidth (%) • Bits per second (bps)
Outgoing Threshold Settings	Enable outgoing thresholds and set the threshold values for the traffic for each port. Units % = Percentage of total bandwidth

Port Security

The Port Security feature applies only to Full firmware. For more information, see Port Security on page 97.

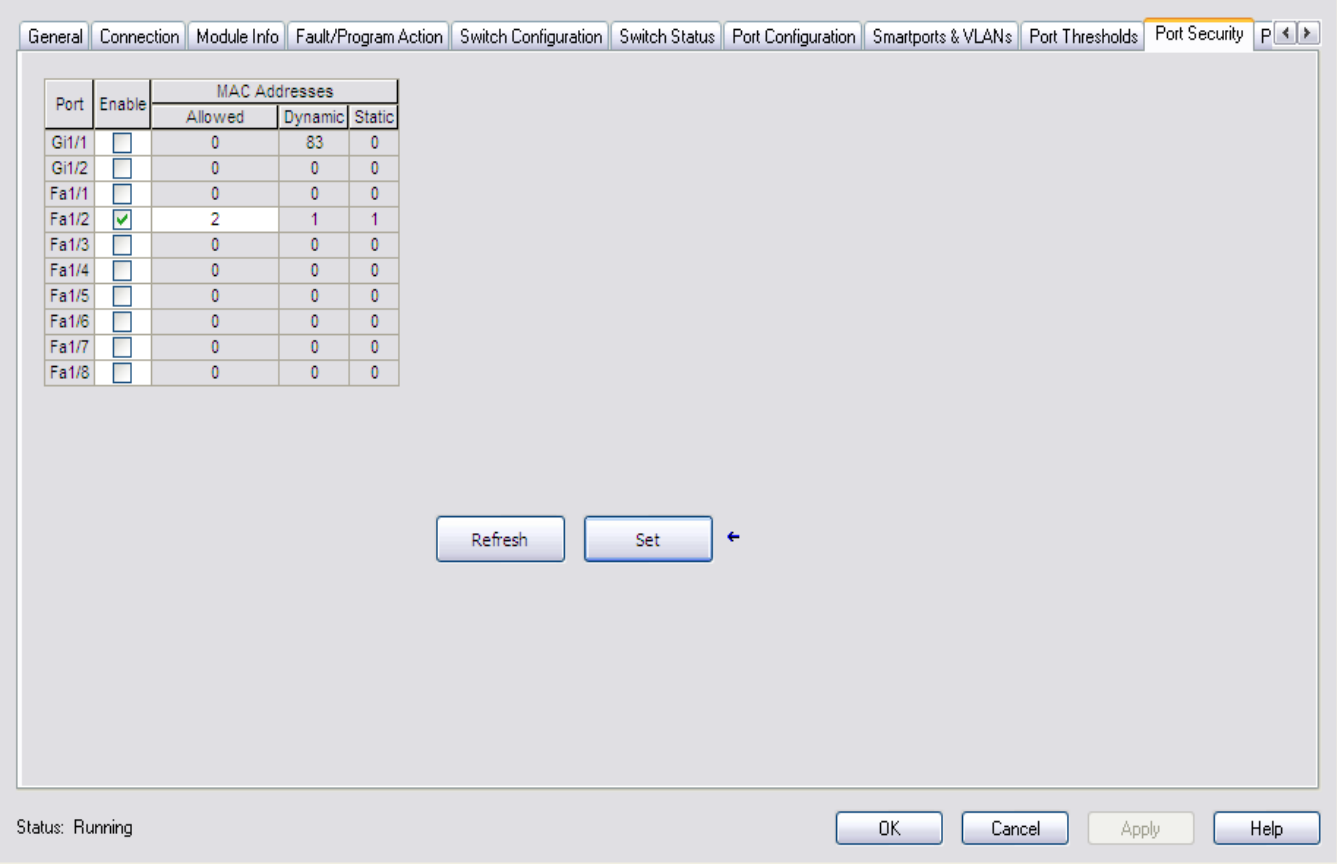


Table 36 - Port Security Tab Fields

Field	Description
Port	The port on which you want to enable or disable security.
Enable	Check the checkbox to enable port security.
MAC Addresses	The number of supported dynamic or static MAC addresses. • Allowed—1…80. • Dynamic—The number of MAC addresses (devices) currently connected to the port that are not manually (statically) defined. • Static—The number of MAC addresses (devices) statically defined by using the Device Manager Web interface. Note that this number must be greater than the sum of the static + dynamic for a given port. If you wish to set the number to less, disconnect the appropriate devices and let their entries in the port security table time out.

Port Status

The Port Status tab lets you monitor alarms, statuses, thresholds, and bandwidth utilization. You can also view port and cable diagnostics.

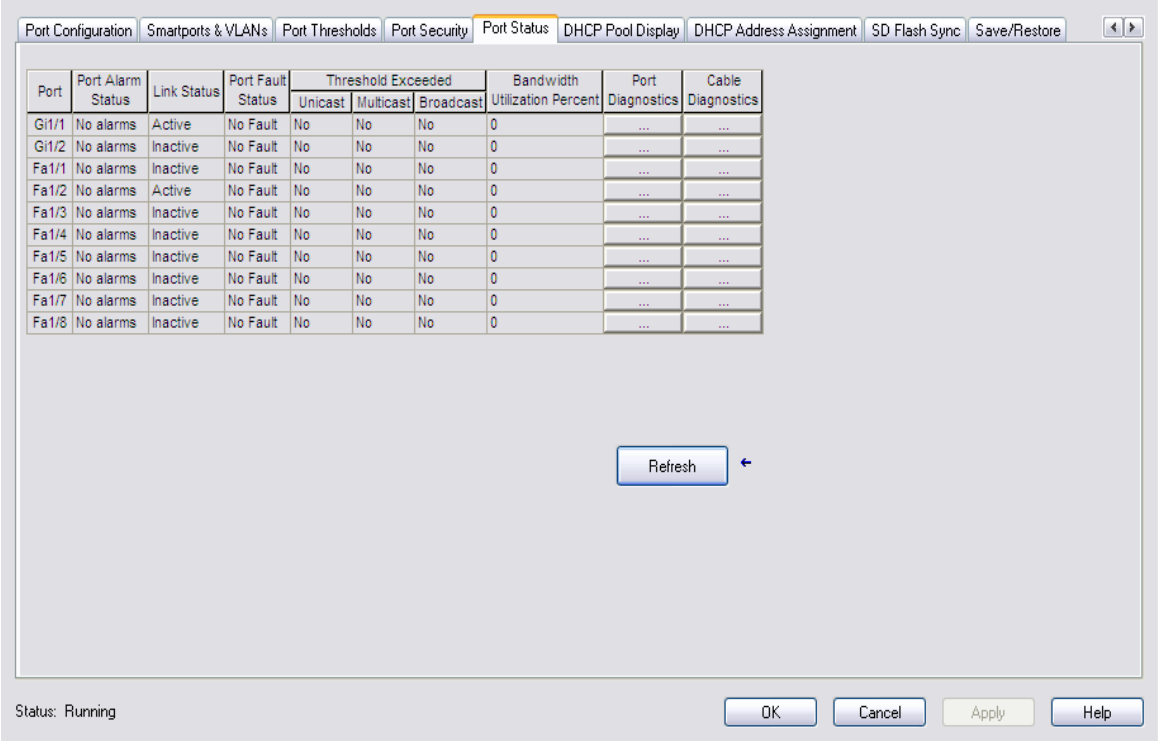

Port Configuration
Smartports & VLANs
Port Thresholds
Port Security
Port Status
DHCP Pool Display
DHCP Address Assignment
SD Flash Sync
Save/Restore
Port
Port Alarm Status
Link Status
Port Fault Status
Threshold Exceeded
Unicast
Multicast
Broadcast
Bandwidth Utilization Percent
Port Diagnostics
Cable Diagnostics
Gi1/1 No alarms Active No Fault No No No 0
Gi1/2 No alarms Inactive No Fault No No No 0
Fa1/1 No alarms Inactive No Fault No No No 0
Fa1/2 No alarms Active No Fault No No No 0
Fa1/3 No alarms Inactive No Fault No No No 0
Fa1/4 No alarms Inactive No Fault No No No 0
Fa1/5 No alarms Inactive No Fault No No No 0
Fa1/6 No alarms Inactive No Fault No No No 0
Fa1/7 No alarms Inactive No Fault No No No 0
Fa1/8 No alarms Inactive No Fault No No No 0
Refresh
Status: Running
OK
Cancel
Apply
Help

Table 37 - Port Status Tab Fields

Field	Description
Port	Displays the selected port. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Port Alarm Status	Displays the current status of the port alarm. Valid values: • Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms
Link Status	Displays whether the link is active or inactive.
Port Fault Status	Displays the current status of the port alarm. Valid values: • Error - Disable event • SFP error - Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault
Threshold Exceeded	Displays unusual changes for these types of network traffic: • Unicast—Displays a yes or no value indicating whether the current unicast traffic has exceeded the threshold value. • Multicast—Displays a yes or no value indicating whether the current multicast traffic has exceeded the threshold value. • Broadcast—Displays a yes or no value indicating whether the current broadcast traffic has exceeded the threshold value.
Bandwidth Utilization Percent	Displays the percentage of the bandwidth being used. Note whether the percentage of usage is what you expect during the given time of network activity. If usage is higher than expected, an issue can exist.
Port Diagnostics	Click to display the Port Diagnostics dialog box for the corresponding port. The Port Diagnostics dialog box provides you information to diagnose a network performance issue.
Cable Diagnostics	Click to display the Cable Diagnostics dialog box for the corresponding port. The Cable Diagnostics dialog box provides information to diagnose a cable issue.

Port Diagnostics

Use the Port Diagnostics dialog box to view the status of the link performance:

- View octet and packet counters
- View collisions on the link
- View errors on the link
- Reset and clear all status counters

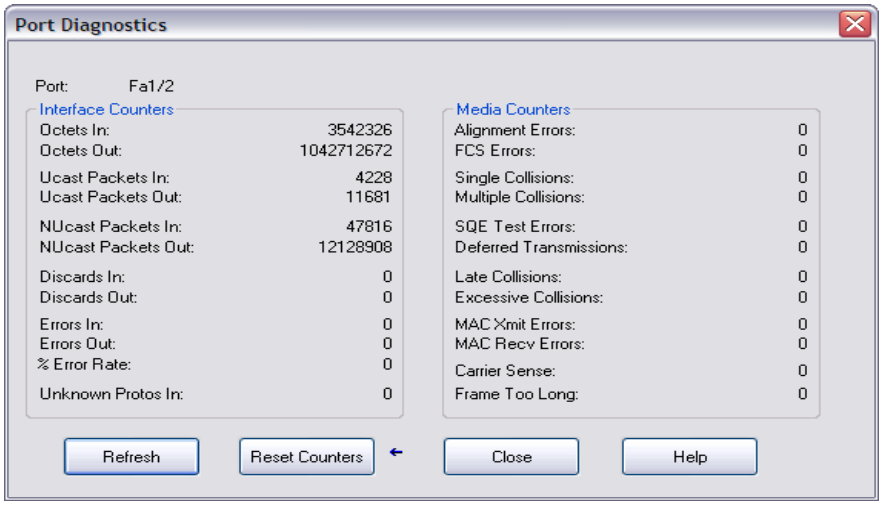
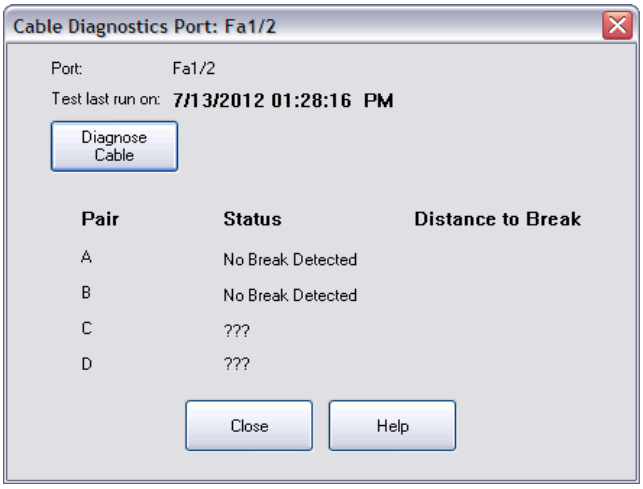


Table 38 - Port Diagnostics Dialog Box Fields

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet) and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Interface Counters	These counters let you view status of octets received and sent, and packets received and sent: • Octets In—The number of octets received by the port. • Octets Out—The number of octets sent by the port. • Ucast Packets In—The number of unicast packets received by the port. • Ucast Packets Out—The number of unicast packets sent by the port. • NUcast packets In—The number of multicast packets received by the port. • NUcast packets Out—The number of multicast packets sent by the port. • Discards In—The number of inbound packets that have been discarded. • Discards Out—The number of outbound packets that have been discarded. • Errors In—The number of inbound packets that contain errors. • Errors Out—The number of outbound packets that contain errors. • Unknown Protos (Protocols) In —The number of inbound packets with unknown protocols.
Media Counters	These counters let you view the number of collisions on a link: • Single—The number of single collisions. • Multiple—The number of multiple collisions. • Late —The number of late collisions. • Excessive—The number of frames for which transmission fails due to excessive collisions. • These counters let you view errors: • Alignment—The number of frames received that are not an integral number of octets in length. • FCS (Frame Check Sequence)—The number of frames received that do not pass the FCS check. • SQE Test Errors —The number of times that the SQE TEST ERROR message is generated. • Deferred Transmissions—The count of transmissions deferred by busy network. • MAC Xmit Errors—The number of frames that failed to transmit due to an internal MAC sublayer transmit error. • MAC Recv Errors—The number of frames that failed to be received due to an internal MAC sublayer receive error. • Carrier Sense—The number of times the carrier sense condition was lost or never asserted when attempting to transmit a frame. • Frame Too Long —The number of frames received that exceed the maximum permitted frame size.

Cable Diagnostics

The Cable Diagnostics dialog box provides information to diagnose a cable issue.



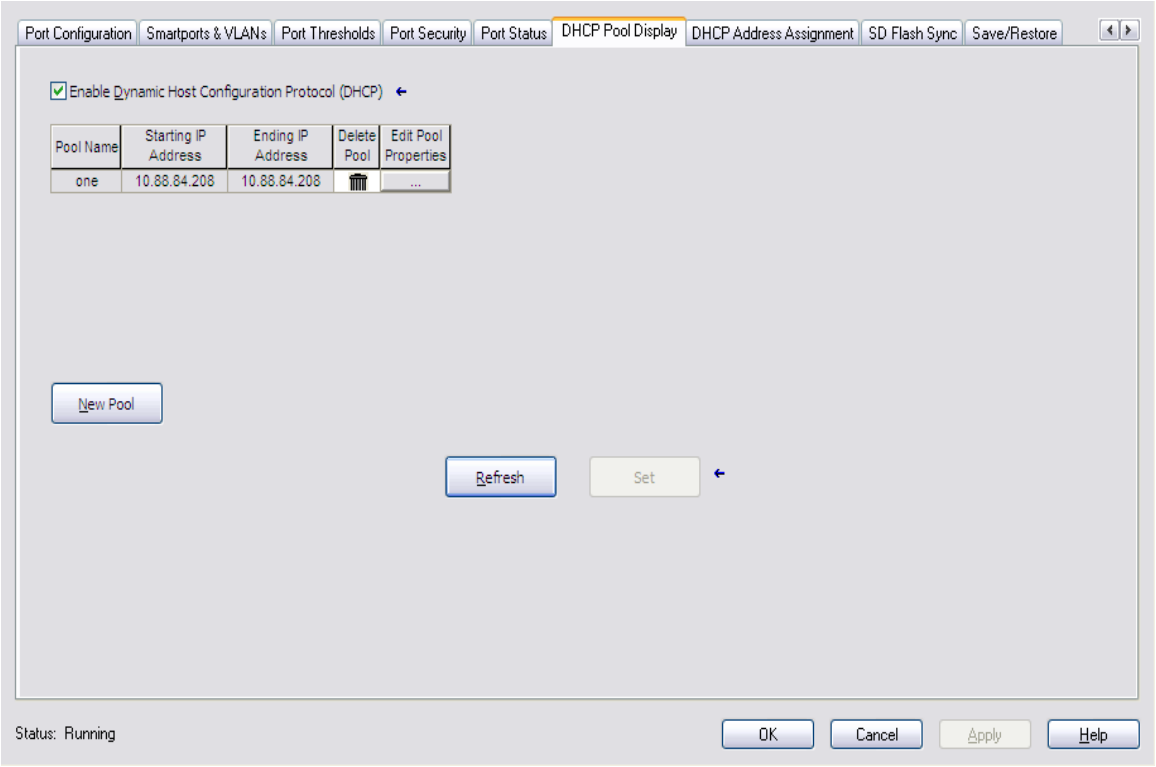
TIP The information on this tab is not displayed if you are offline.

Table 39 - Cable Diagnostics Port Dialog Box Fields

Field	Description
Port	The port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Test last run on	The time the test was last executed. The date time format is mm/dd/yy hh:mm:ss tt. If the test has never been run, the time and all distance and status information is blank.
Pair	Each pair (pair of cables in the network) individually listed. If pair does not exist or test has never been run, this is blank.
Status	Specifies the link state the last time the test was executed. If pair does not exist or test has never run, status is blank. For distance, if the pair is Normal status, 'No Break Detected' is shown. No distance is displayed.
Distance to Break	The distance to the break from the switch for each estimated pair with a plus or minus error value individually listed. A value is displayed only when the status of an existing pair is not Normal. This is blank if the test was never run before. If a pair does not exist, '???' appears.
Diagnose Cable	Click to run the Diagnose Cable test. A connection interruption warning appears: • If you are sure you want to continue with the test, click Yes. Be prepared to enter a valid password to run the test. • If you do not want to run the test, click No or close the window. **IMPORTANT:** To run a valid test on gigabit ports, you must first configure the gigabit port as an RJ45 media type in the Device Manager Web interface, as described in Configure Port Settings on page 132. **IMPORTANT:** This test can interrupt connections to the module and to any other modules connected through this module. Also, the connection between workstation and controller can be interrupted. You must have the correct privilege to run this test.

DHCP Pool Display

You can view DHCP address pool information for the switch from the DHCP Pool Display tab. You can view 0...15 pools. This information is gathered directly from the switch. Each row represents a single instance, and instance values cannot be consecutive.



TIP The information on this tab is not displayed if you are offline.

Table 40 - DHCP Pool Dislay Tab Fields

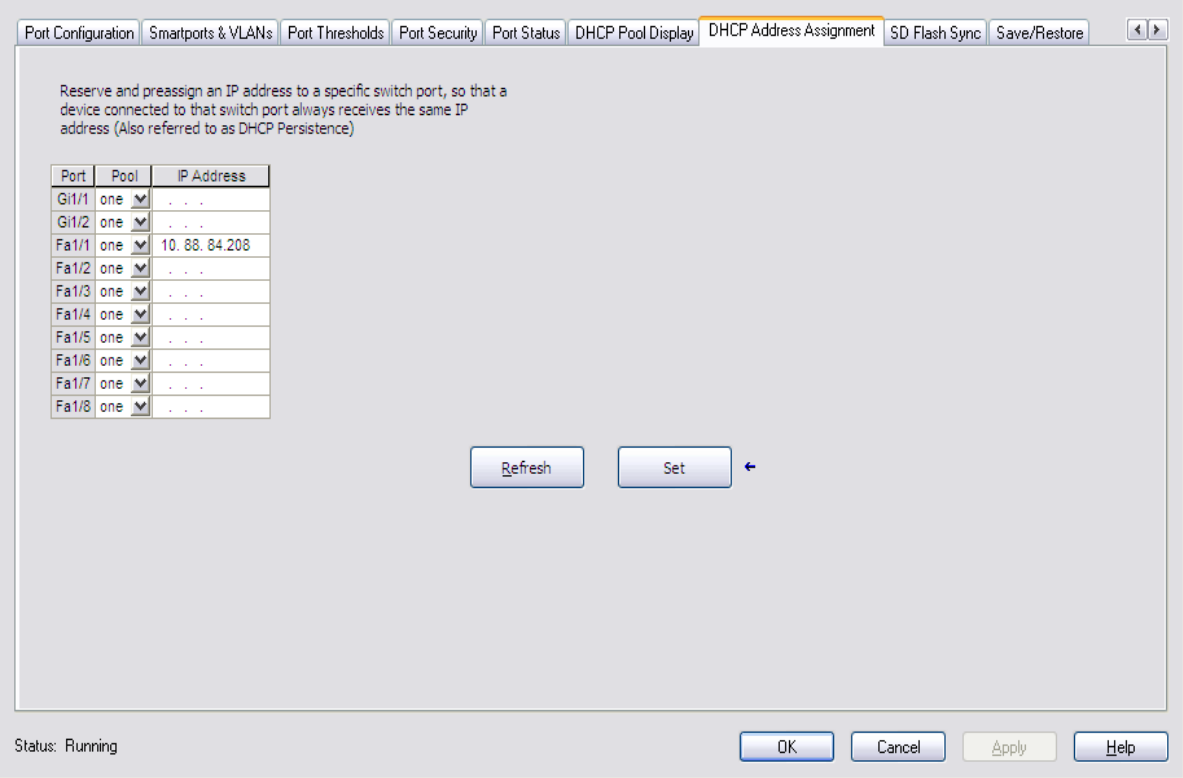
Field	Description
Enable Dynamic Host Configuration Protocol (DHCP)	Enables or disables pools. If selected, all controls on the grid are set to online and the appropriate values are obtained from the switch and displayed. If cleared, all controls on the grid are set to offline. From the keyboard, press Alt - D.
Pool Name	Displays the name of the DHCP IP address pool configured on the switch. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
Starting IP Address	Displays the starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Ending IP Address	Displays the ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0…255.
Delete Pool	Click to delete currently selected DHCP pool row. Afterwards, if you click Set, a confirmation dialog box is displayed and all of the persistent addresses associated with the selected DHCP pool row are also deleted. Delete Pool is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is checked, and when the respective row is populated. Delete Pool is dimmed when the switch is offline, and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
Refresh	Click to refresh the grid control with new data obtained directly from the switch. From the keyboard, press Alt-R. If you have changed a value in the grid and clicked Refresh before clicking Set, all values in the grid are returned to their previously set values. Refresh is available only when the switch is online. The Refresh button is dimmed when the switch is offline.

Table 40 - DHCP Pool Dislay Tab Fields (continued)

Field	Description
Edit Pool Properties	Click to display the DHCP Pool Definition and Edit dialog box and populate it with values from the instance corresponding to the current row. The Edit column button is available only when the switch is online, the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is selected, and when the respective row is populated. The Edit column button is dimmed when the switch is offline and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
New Pool	Click to display the DHCP Pool Definition and Edit dialog box (all fields are blank and the Custom radio button is not selected). Additionally, a new row/instance is added to the grid on the Module Properties dialog box - DHCP Pool Display. From the keyboard, press Alt - N. The New button is available only when the switch is online and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is selected. The New button is dimmed when the switch is offline and the Enable Dynamic Host Configuration Protocol (DHCP) checkbox is cleared.
Set	Click to apply attribute changes on this dialog box to the switch. Only those attributes that have been modified are applied to the switch. The Enter Password dialog box can appear. If an error occurs while setting an attribute, the Set operation is terminated and all subsequent attribute values are not applied to the switch. Additionally, the Set button remains available. The Set button is available only when the switch is online and any of the attribute values have changed. The Set button is dimmed when the switch is offline.

DHCP Address Assignment

You can view and configure DHCP persistence from the DHCP Address Assignment tab. With DHCP persistence, you can assign a specific IP address to each port, so that the device attached to a specific port receives the same IP address.



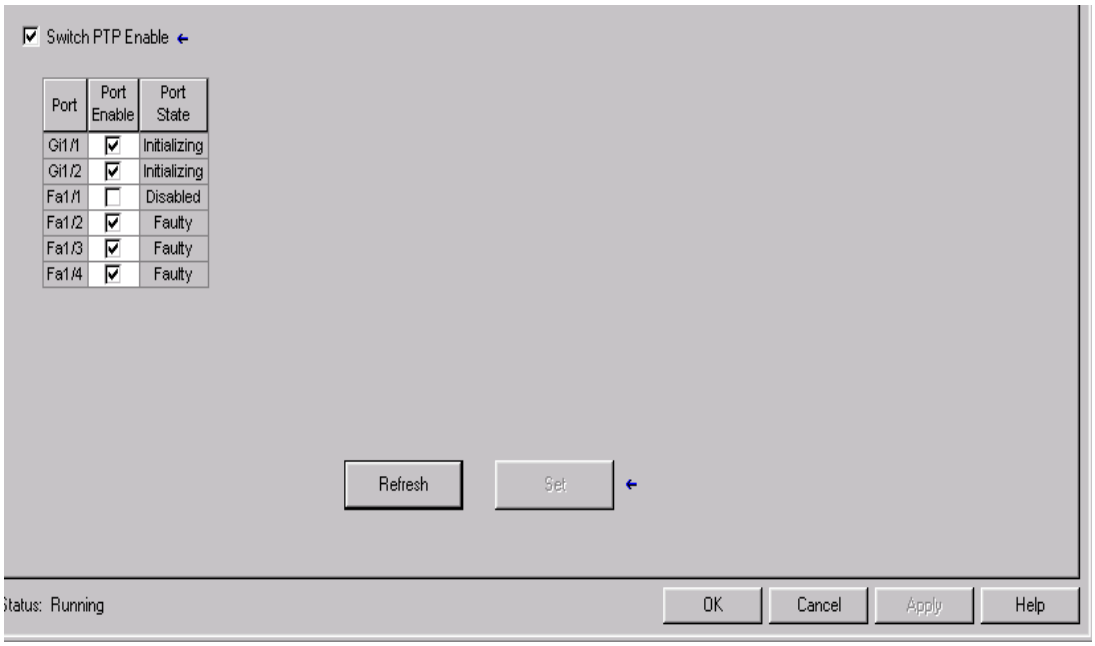
TIP The information on this tab is not displayed if you are offline.

Table 41 - DHCP Address Assignment Tab Fields

Field	Description
Port	Displays the ports available for the configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the switch number (1), and the specific port number. **EXAMPLE:** • Gi1/1 is Gigabit Ethernet port 1. • Fa1/1 is Fast Ethernet port 1.
Pool	Displays the pool names from the DHCP IP address pool that corresponds to the instances available in the switch. If you delete all of the rows containing pools on the DHCP Pool Display tab on the Module Properties dialog box and click Refresh, the Pool field is blank. The Pool field is available when the switch is online and appears dimmed when the switch is offline.
IP Address	Displays the IP address assigned to the switch port. The format is a 32-bit numeric address written as four numbers separated by periods (for example, 255.255.255.255). Each number can be from 0 . . . 255. IP Address is available only when the switch is online and dimmed when the switch is offline.
Refresh	Click to refresh the grid control with new data obtained directly from the switch. From the keyboard, press Alt-R. If you have changed a value in the grid and clicked Refresh before clicking Set, all values in the grid are returned to their previously set values. The Refresh button is available only when the switch is online. The Refresh button is dimmed when the switch is offline.
Set	Click to apply changes on this dialog box to the switch. The Enter Password dialog box can appear.

Time Sync Configuration

Use this feature to synchronize the ports through PTP. PTP synchronizes with nanosecond accuracy the real-time clocks of the devices in a network. By using the best master clock selection, the switch identifies the switch port that is connected to a device with the best clock source. The switch then synchronizes its internal clock with the best clock source and the switch port is set to master state. The most precise clock source in the network is referred to as the grandmaster clock. For more information about this feature, see CIP Sync Time Synchronization (Precision Time Protocol) on page 100.



TIP The information on this tab is not displayed if you are offline.

Table 42 - Time Sync Configuration Tab Fields

Field	Description
Switch PTP Enable	Check to enable the PTP on the device. By default, PTP is enabled on all of the Fast Ethernet and Gigabit Ethernet ports on the switch. Clear the checkbox to disable the PTP on the device. The Port Enable and Port State features appear dimmed when the Switch PTP Enable checkbox is cleared.
Port	Displays the port selected for configuration. The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), and the specific port number. **EXAMPLE:** Gi1/1 is Gigabit Ethernet port 1.
Port Enable	Check to enable the configuration of the port on the device. Clear the checkbox to disable the port configuration on the device. The Port Enable feature appears dimmed when the Switch PTP Enable checkbox is cleared.
Port State	Displays the current state of the PTP port on the device. Valid values: • Initializing • Faulty • Disabled • Listening • Pre-Master • Master • Uncalibrated • Slave The Port State field is blank and dimmed when the Switch PTP Enable checkbox is cleared.
Refresh	Click to refresh the tab with new data from the switch.
Set	Click to send the settings to the switch. The Enter Password dialog box can appear. Be prepared to enter a valid password to set configuration settings. The Set button appears dimmed when the switch is offline.

NAT Configuration

You can create NAT instances from the NAT tab.

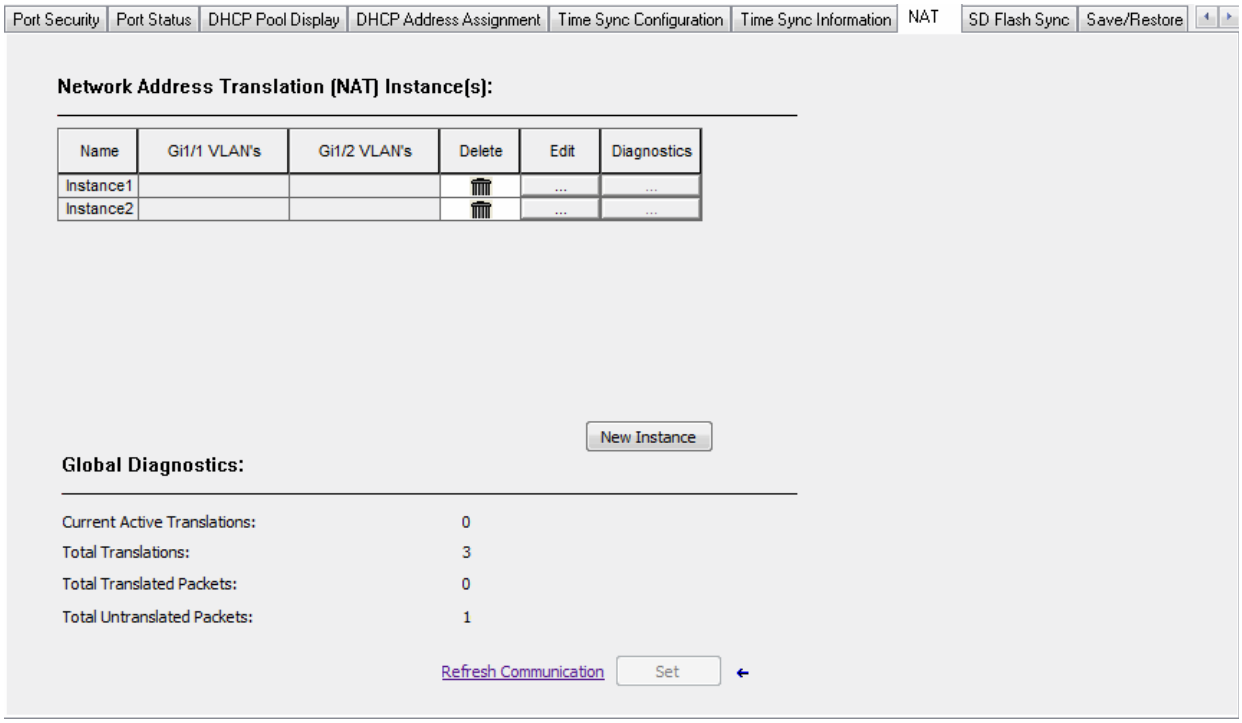


Table 43 - NAT Tab Fields

Field	Description
Name	Displays the unique name of the NAT instance.
Gi1/1 VLANs	Displays the VLANs assigned to each NAT instance on port Gi1/1.
Gi1/2 VLANs	Displays the VLANs assigned to each NAT instance on port Gi1/2.
Delete	Click to permanently delete a NAT instance. The switch deletes the instance when you click Set.
Edit	Click to modify the configuration of a NAT instance.
Diagnostics	Click to view translation diagnostics for an instance. See page 229.
New Instance	Click to create a NAT instance. See page 216.
Current Active Translations	Displays the total number of translations that occurred within the last 90 seconds across all NAT instances.
Total Translations	Displays the total number of translations across all NAT instances.
Total Translated Packets	Displays the total number of translated packets across all NAT instances.
Total Untranslated Packets	Displays the total number of packets that have been bypassed across all NAT instances.
Refresh Communication	Click to refresh all data on the tab.
Set	Click to delete a NAT instance from the switch after clicking the Trash icon next to the instance.

To configure NAT, follow one of these procedures based on your application:

- Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

  For an example of this application, see Figure 4 on page 102.
- Create NAT Instances for Traffic Routed through a Layer 2 Switch

  For an example of this application, see Figure 5 on page 103.

IMPORTANT Set up all Smartport roles and VLANs before creating NAT instances.

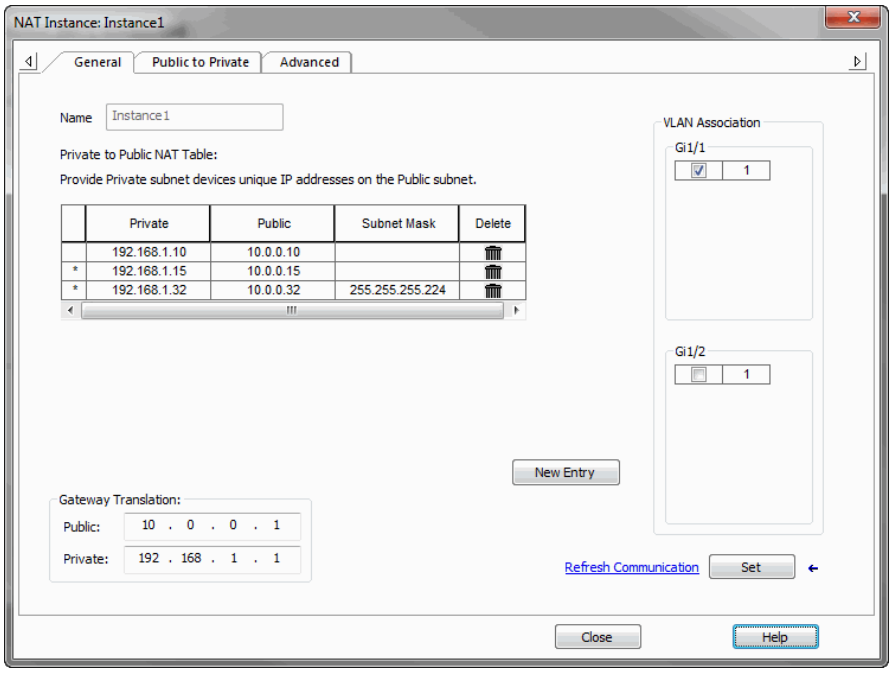
If you change a Smartport role or the native VLAN for a port associated with a NAT instance, you must reassign VLANs to the NAT instance.

IMPORTANT As a result of Layer 2 forwarding, current traffic sessions remain established until manually disconnected. If you change an existing translation, you must manually disconnect all associated traffic sessions before the new translation can take effect.

Create NAT Instances for Traffic Routed through a Layer 3 Switch or Router

To create a NAT instance for traffic routed through a Layer 3 switch or router, follow these steps.

1. From the NAT tab, click New Instance to display the General tab of the NAT Instance dialog box.



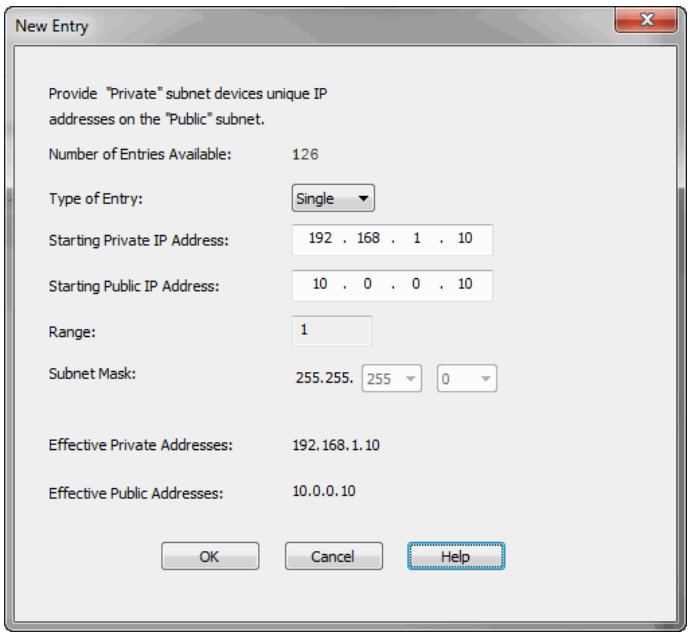
2. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

3. In the VLAN Association area, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 105.

4. Click New Entry to display the New Entry dialog box.



5. Do one of the following:
   - To translate a single address for a device on the private subnet that needs to communicate on the public subnet, complete the fields below.

Field	Description
Type of Entry	Choose Single. This is the default value.
Starting Private IP Address	Type the existing address for the device on the private subnet.
Starting Public IP Address	Type a unique public address to represent the device.
Effective Private Addresses	Displays the existing address for the device on the private subnet that is configured for translation. If blank, verify that the values in the fields above are valid.
Effective Public Addresses	Displays the unique public address to represent the device. If blank, verify that the values in the fields above are valid.

   - To translate a range of addresses for devices on the private subnet that need to communicate on the public subnet, complete the fields below.

Field	Description
Type of Entry	Choose Range.
Starting Private IP Address	Type the existing starting address for the device on the private subnet.
Starting Public IP Address	Type a unique, starting public address to represent the device.
Range	Type the number of addresses to include in the range. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the fields above are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the fields above are valid.

- To translate all of the addresses in the private subnet or a portion of the private subnet, complete the fields below.

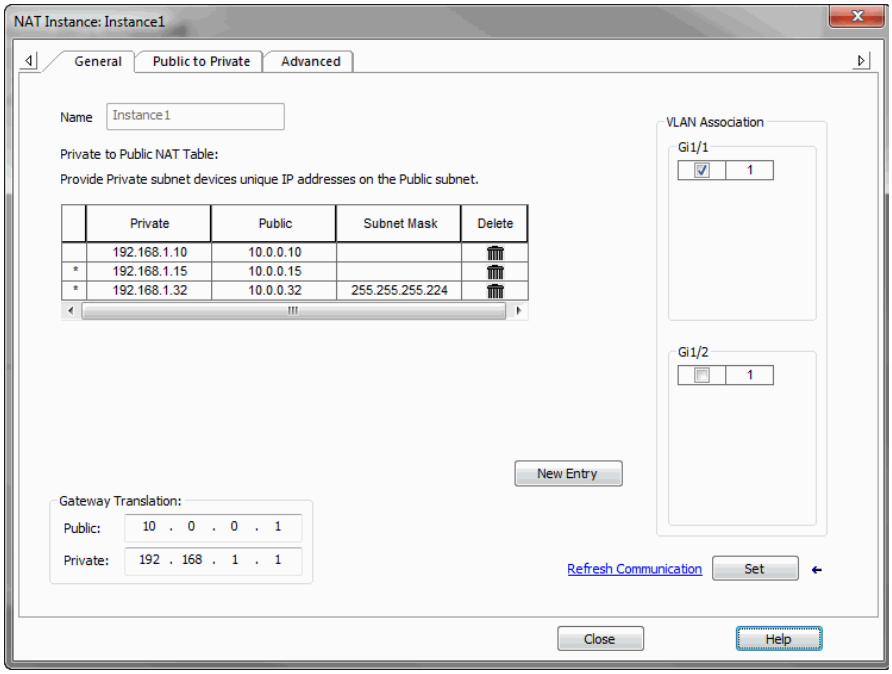
Field	Description	
Type of Entry	Choose Subnet.	
Starting Private IP Address	Type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16
Starting Public IP Address	Type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16
Subnet Mask	From the pull-down menus, choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)	
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the fields above are valid.	
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the fields above are valid.	

6. Click OK.
7. Complete the Gateway Translation fields to enable devices on the public subnet to communicate with devices on the private subnet:
   - Public—Type the default gateway address of the Layer 3 switch or router connected to the switch's uplink port.
   - Private—Type a unique IP address to represent the Layer 3 switch or router on the private network.
8. To configure traffic permits and packet fixups, proceed to Configure Traffic Permits and Fixups on page 228.
9. Click Set.

Create NAT Instances for Traffic Routed through a Layer 2 Switch

To create a NAT instance for traffic routed through a Layer 2 switch, follow these steps.

1. From the NAT tab, click New Instance to display the NAT Instance dialog box.



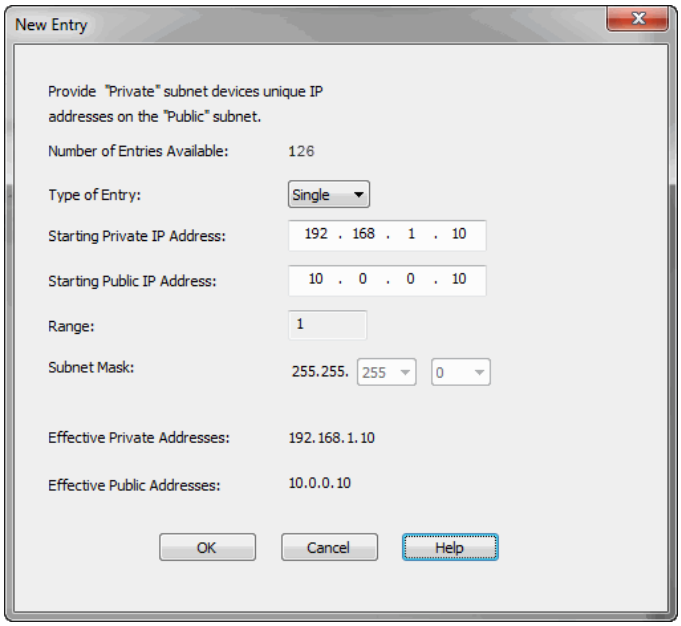
2. In the Name field, type a unique name to identify the instance.

   The instance name cannot include spaces or exceed 32 characters.

3. From the list of VLANs on the right, check the checkbox next to each VLAN to assign to the instance.

   For more information about VLAN assignments, see page 105.

4. Click New Entry to display the New Entry dialog box.



5. Do one of the following:
   - To translate a single address for a device on the private subnet that needs to communicate on the public subnet, complete the fields below.

Field	Description
Type of Entry	Choose Single. This is the default value.
Starting Private IP Address	Type the existing address for the device on the private subnet.
Starting Public IP Address	Type a unique public address to represent the device.
Effective Private Addresses	Displays the existing address for the device on the private subnet that is configured for translation. If blank, verify that the values in the fields above are valid.
Effective Public Addresses	Displays the unique public address to represent the device. If blank, verify that the values in the fields above are valid.

   - To translate a range of addresses for devices on the private subnet that need to communicate on the public subnet, complete the fields below.

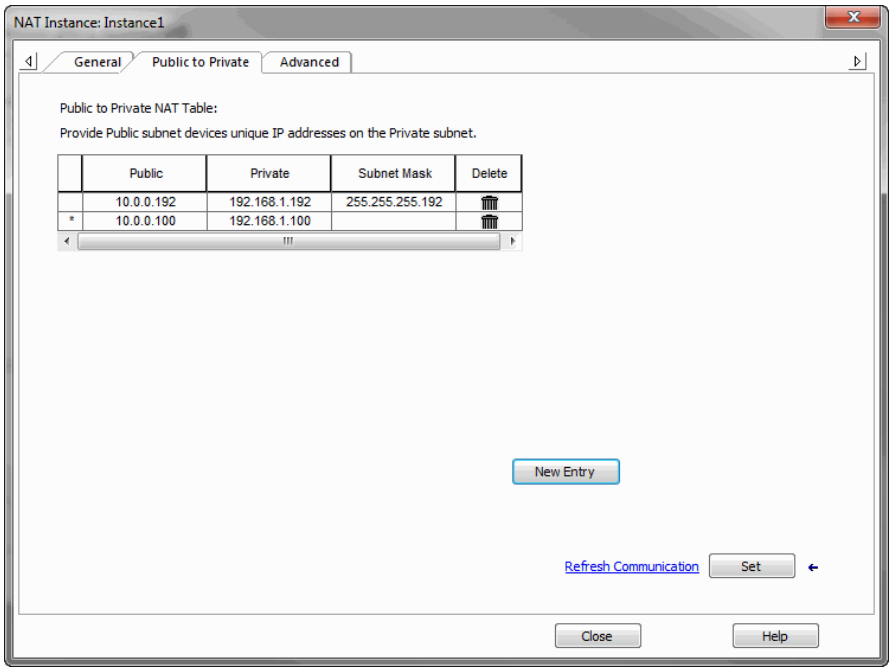
Field	Description
Type of Entry	Choose Range.
Starting Private IP Address	Type the existing starting address for the device on the private subnet.
Starting Public IP Address	Type a unique, starting public address to represent the devices.
Range	Type the number of addresses to include in the range. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the fields above are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the fields above are valid.

- To translate all of the addresses in the private subnet or a portion of the private subnet, complete the fields as described in the table below.

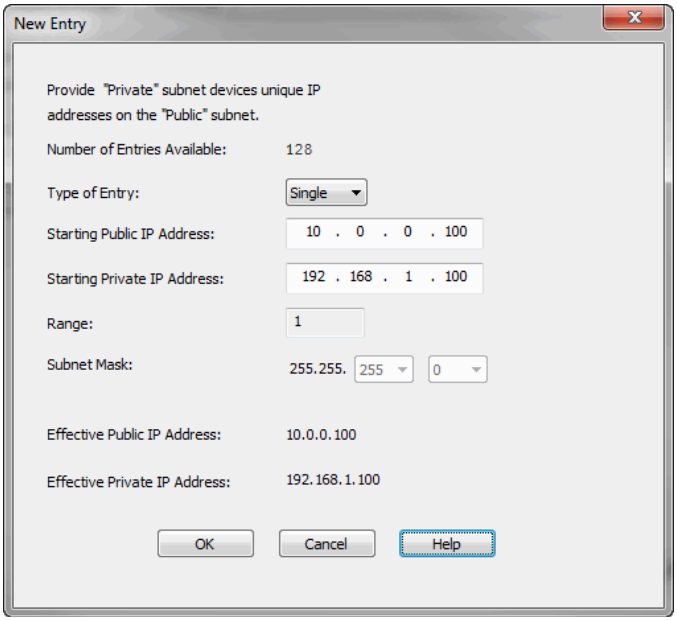
Field	Description	
Type of Entry	Choose Subnet.	
Starting Private IP Address	Type the existing starting address for a device on the private subnet. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16
Starting Public IP Address	Type a unique, starting public address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16

Field	Description
Subnet Mask	From the pull-down menus, choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)
Effective Private Addresses	Displays the range of existing addresses for devices on the private subnet that are configured for translation. If blank, verify that the values in the fields above are valid.
Effective Public Addresses	Displays the range of unique public addresses to represent the devices. If blank, verify that the values in the fields above are valid.

6. Click OK.
7. Click the Public to Private tab.



8. Click New Entry to display the New Entry dialog box.



9. Do one of the following:

- To translate a single address for a device on the public subnet that needs to communicate on the private subnet, complete the fields below.

Field	Description
Type of Entry	Choose Single. This is the default value.
Starting Public IP Address	Type the existing address for the device on the public subnet.
Starting Private IP Address	Type a unique private address to represent the device.
Effective Public Addresses	Displays the existing address for the device on the public subnet that is configured for translation. If blank, verify that the values in the fields above are valid.
Effective Private Addresses	Displays the unique private address to represent the device. If blank, verify that the values in the fields above are valid.

- To translate a range of addresses for devices on the public subnet that need to communicate on the private subnet, complete the fields below

Field	Description
Type of Entry	Choose Range.
Starting Public IP Address	Type the existing starting address for the device on the public subnet.
Starting Private IP Address	Type a unique, starting private address to represent the devices.
Range	Type the number of addresses to include in the range. Valid values: 1…128 Default value = 1 **IMPORTANT:** Each address in the range counts as one translation entry. The switch supports a maximum of 128 translation entries.
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the fields above are valid.
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the fields above are valid.

- To translate all of the addresses in the public subnet or a portion of the public subnet, complete the fields as described in the table below.

Field	Description	
Type of Entry	Choose Subnet.	
Starting Public IP Address	Type the existing starting address for a device on the public subnet. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Public Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 10.200.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 10.200.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 10.200.1.0 or 10.200.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 10.200.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 10.200.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 10.200.1.16
Starting Private IP Address	Type a unique, starting private address to represent the devices. This address must correspond to the size of the subnet mask to translate as shown below.	
	Subnet Mask	**Starting Private Subnet Address**
	255.255.0.0	The last two octets must end in 0. **EXAMPLE:** 192.168.0.0
	255.255.255.0	The last octet must end in 0. **EXAMPLE:** 192.168.1.0
	255.255.255.128	The last octet must end in 0 or 128. **EXAMPLE:** 192.168.1.0 or 192.168.1.128
	255.255.255.192	The last octet must in one of the following: 0, 64, 128, 192. **EXAMPLE:** 192.168.1.64
	255.255.255.224	The last octet must in one of the following: 0, 32, 64, 96, 128, 160, 192, 224. **EXAMPLE:** 192.168.1.32
	255.255.255.240	The last octet must in one of the following: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXAMPLE:** 192.168.1.16

Field	Description
Subnet Mask	From the pull-down menus, choose the subnet mask for the addresses to translate. Valid values: • Class B: 255.255.0.0 • Class C: 255.255.255.0 • Portion of Class C: – 255.255.255.128 (provides 128 addresses per translation entry – 255.255.255.192 (provides 64 addresses per translation entry – 255.255.255.224 (provides 32 addresses per translation entry – 255.255.255.240 (provides 16 addresses per translation entry)
Effective Public Addresses	Displays the range of existing addresses for devices on the public subnet that are configured for translation. If blank, verify that the values in the fields above are valid.
Effective Private Addresses	Displays the range of unique private addresses to represent the devices. If blank, verify that the values in the fields above are valid.

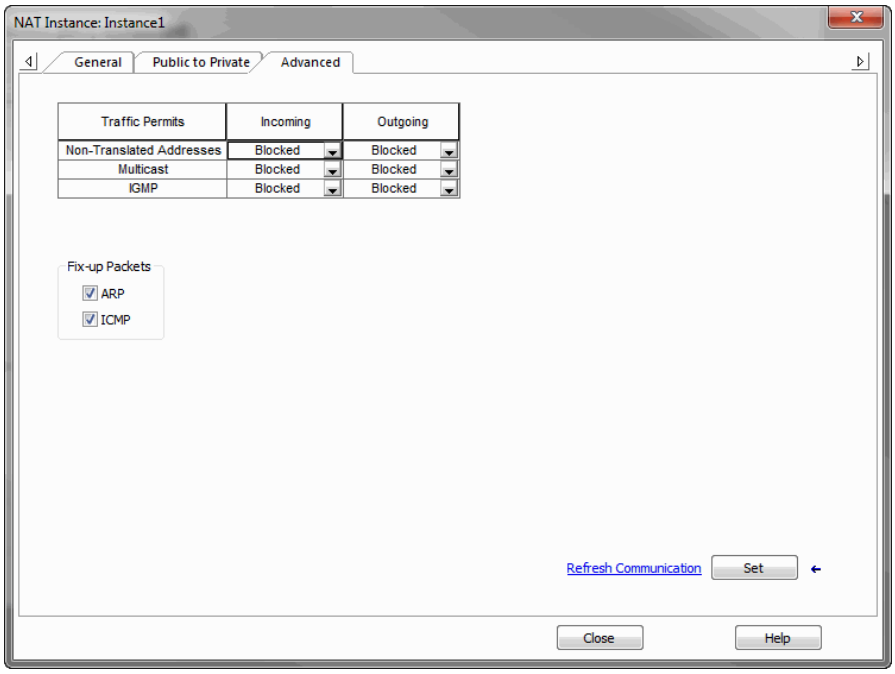
10. Click OK.
11. (Optional). To configure traffic permits and packet fixups, proceed to Configure Traffic Permits and Fixups on page 228.
12. Click Set.

Configure Traffic Permits and Fixups

Use caution when configuring traffic permits and fixups. We recommend you use the default values.

To configure traffic permits or packet fixups, follow these steps.

1. Click the Advanced tab.



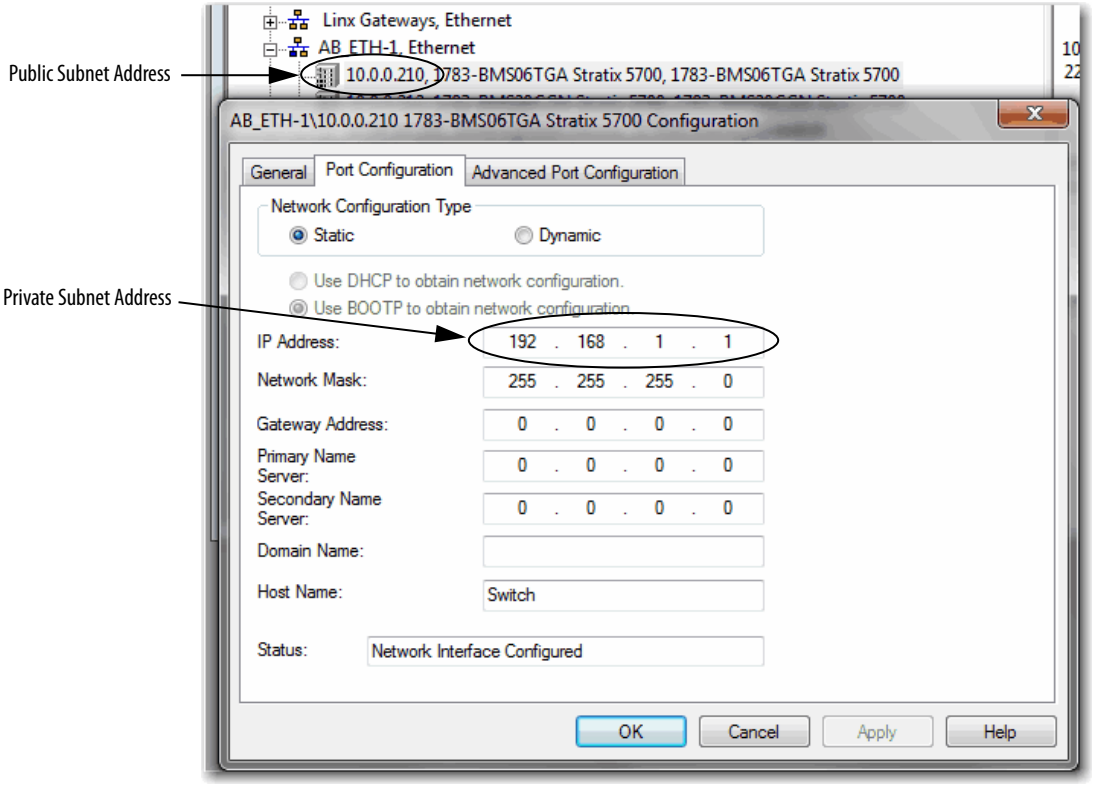
2. In the Traffic Permits grid, choose one of these options for incoming and outgoing packets that are not handled by NAT:
   - Pass-Through—Permit the packets to pass across the NAT boundary.
   - Blocked—Drop the packets.
3. In the Fix-up Packets area, check or clear the checkboxes to enable or disable protocol fixups for ARP and ICMP.

   By default, fixups are enabled for both ARP and ICMP.

View Address Translations in RSLinx Software

The Ethernet driver in RSLinx software supports devices with address translations. If a device's address is configured for translation, its public subnet address appears on the main dialog box of RSLinx sofware. However, its private subnet address appears in the device's configuration properties.

Figure 9 - Public and Private Subnet Addresses in RSLinx Software

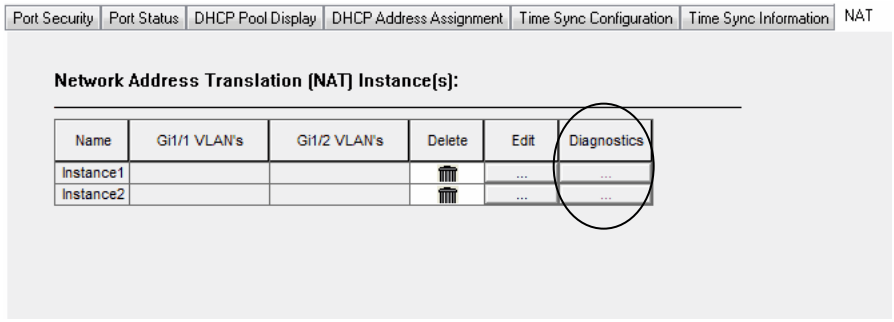

Public Subnet Address
Private Subnet Address
Linx Gateways, Ethernet
AB_ETH-1, Ethernet
10.0.0.210, 1783-BMS06TGA Stratix 5700, 1783-BMS06TGA Stratix 5700
AB_ETH-1\10.0.0.210 1783-BMS06TGA Stratix 5700 Configuration
General
Port Configuration
Advanced Port Configuration
Network Configuration Type
Static
Dynamic
Use DHCP to obtain network configuration.
Use BOOTP to obtain network configuration.
IP Address: 192 . 168 . 1 . 1
Network Mask: 255 . 255 . 255 . 0
Gateway Address: 0 . 0 . 0 . 0
Primary Name Server: 0 . 0 . 0 . 0
Secondary Name Server: 0 . 0 . 0 . 0
Domain Name:
Host Name: Switch
Status: Network Interface Configured
OK
Cancel
Apply
Help

NAT Diagnostics

For each NAT instance, you can monitor these diagnostics:

- Diagnostics for both private and public translations
- Diagnostics for only private translations
- Diagnostics for only public translations

To access diagnostics for an instance, from the NAT tab, click the ellipse in the Diagnostics column.



The NAT Diagnostics dialog box displays diagnostics for the selected instance.

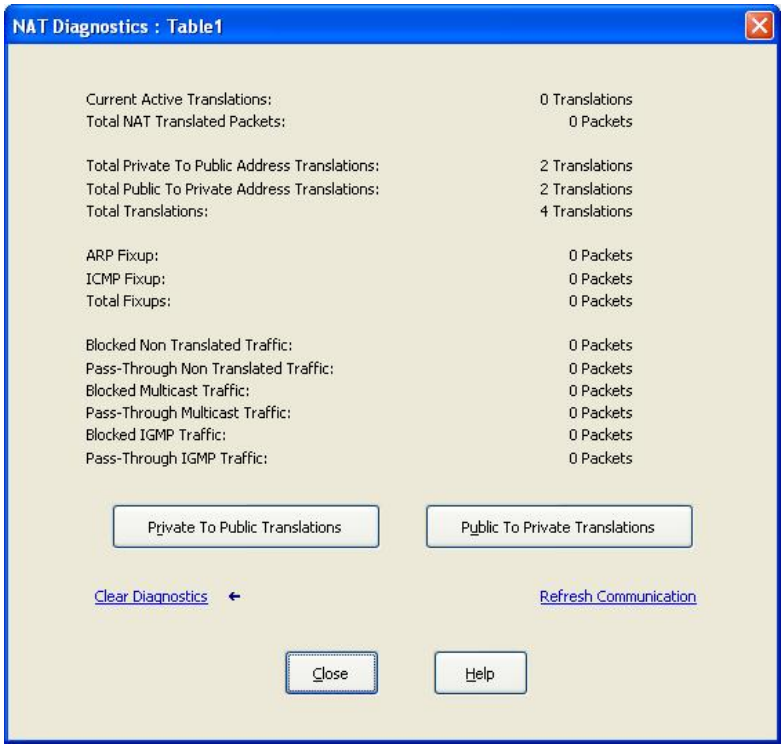

NAT Diagnostics : Table1
Current Active Translations: 0 Translations
Total NAT Translated Packets: 0 Packets
Total Private To Public Address Translations: 2 Translations
Total Public To Private Address Translations: 2 Translations
Total Translations: 4 Translations
ARP Fixup: 0 Packets
ICMP Fixup: 0 Packets
Total Fixups: 0 Packets
Blocked Non Translated Traffic: 0 Packets
Pass-Through Non Translated Traffic: 0 Packets
Blocked Multicast Traffic: 0 Packets
Pass-Through Multicast Traffic: 0 Packets
Blocked IGMP Traffic: 0 Packets
Pass-Through IGMP Traffic: 0 Packets
Private To Public Translations
Public To Private Translations
Clear Diagnostics
Refresh Communication
Close
Help

Table 44 - NAT Diagnostics per Instance

Field	Description
Current Active Translations	Displays the number of translations that have occurred within the last 90 seconds across all NAT instances.
Total NAT Translated Packets	Displays the total number of packets that have been translated for this instance.
Total Private to Public Address Translations	Displays the total number of private-to-public translations for this instance.
Total Public to Private Address Translations	Displays the total number of public-to-private translations for this instance.
ARP Fixup	Displays the number of ARP packets that have been fixed up for this instance.
ICMP Fixup	Displays the number of ICMP packets that have been fixed up for this instance.
Total Fixups	Displays the number of ARP and ICMP packets that have been fixed up for this instance.
Incoming Non Translated Traffic (Pass-Through)	Displays the number of incoming packets with untranslated traffic that NAT passed through for this instance.
Outgoing Non Translated Traffic (Blocked)	Displays the number of outgoing packets with untranslated traffic that NAT blocked for this instance.
Incoming Multicast Traffic (Blocked)	Displays the number of incoming packets with multicast traffic that NAT blocked for this instance.
Outgoing Multicast Traffic (Pass-Through)	Displays the number of outgoing packets of multicast traffic that NAT passed through for this instance.
Incoming IGMP Traffic (Blocked)	Displays the number of incoming packets with IGMP traffic that NAT blocked for this instance.
Outgoing IGMP Traffic (Blocked)	Displays the number of outgoing packets with IGMP traffic that NAT blocked for this instance.
Private to Public Translations	Click to view private-to-public translation diagnostics for the instance. See Private-to-Public Translation Diagnostics on page 231.
Public to Private Translations	Click to view private-to-public translation diagnostics for the instance. See Public-to-Private Translation Diagnostics on page 232.
Refresh Communication	Click to refresh all diagnostics for this instance.

Private-to-Public Translation Diagnostics

From the Private to Public Translations dialog box for an instance, you can view a list of IP addresses that have been changed by NAT within the last 90 seconds.

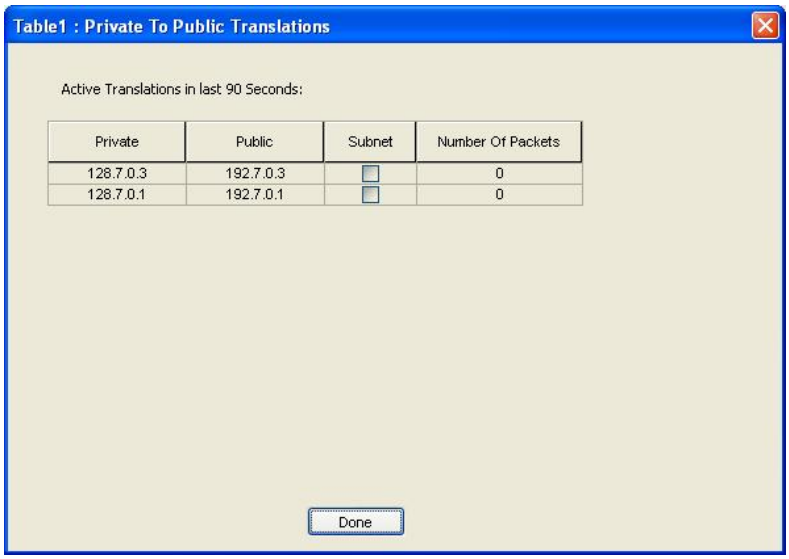


Table 45 - Private-to-Public Translation Diagnostics

Field	Description
Private	Displays the existing address for a device on the private subnet.
Public	Displays a unique public address that represents the corresponding device on the private subnet.
Subnet	Indicates whether the translation is part of a Subnet entry type.
Number of Packets	Displays the number of packets that contain the translation.

Public-to-Private Translation Diagnostics

From the Public to Private Translations dialog box for an instance, you can view a list of IP addresses that have been changed by NAT within the last 90 seconds.

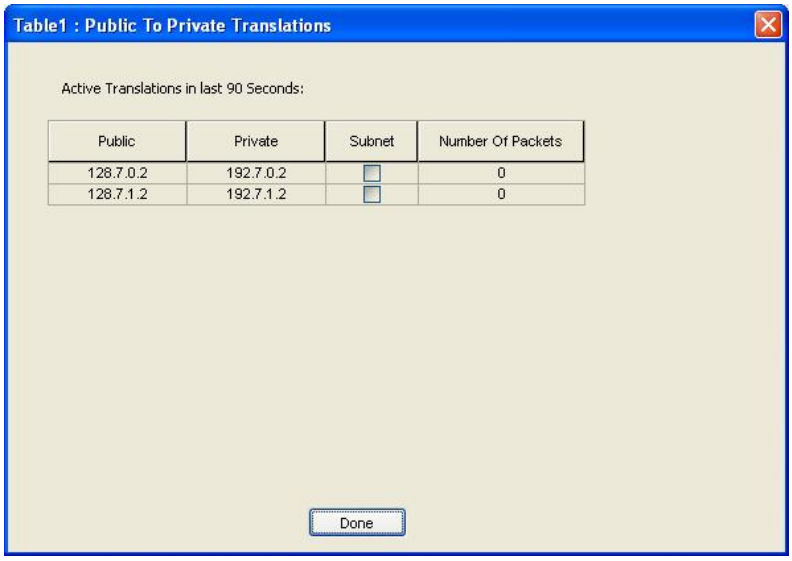


Table 46 - Public-to-Private Translation Diagnostics

Field	Description
Public	Displays the unique IP address on the public subnet that represents the corresponding IP address on the private subnet.
Private	Displays the IP address on the private subnet that was changed to a unique IP address on the public subnet.
Subnet	Indicates whether the translation is part of a Subnet entry type.
Number of Packets	Displays the number of packets that contain the translation.

SD Flash Sync

You can sync the SD card to either the configuration file or the entire image.

IMPORTANT You can overwrite your configuration if you synchronize in the wrong direction.

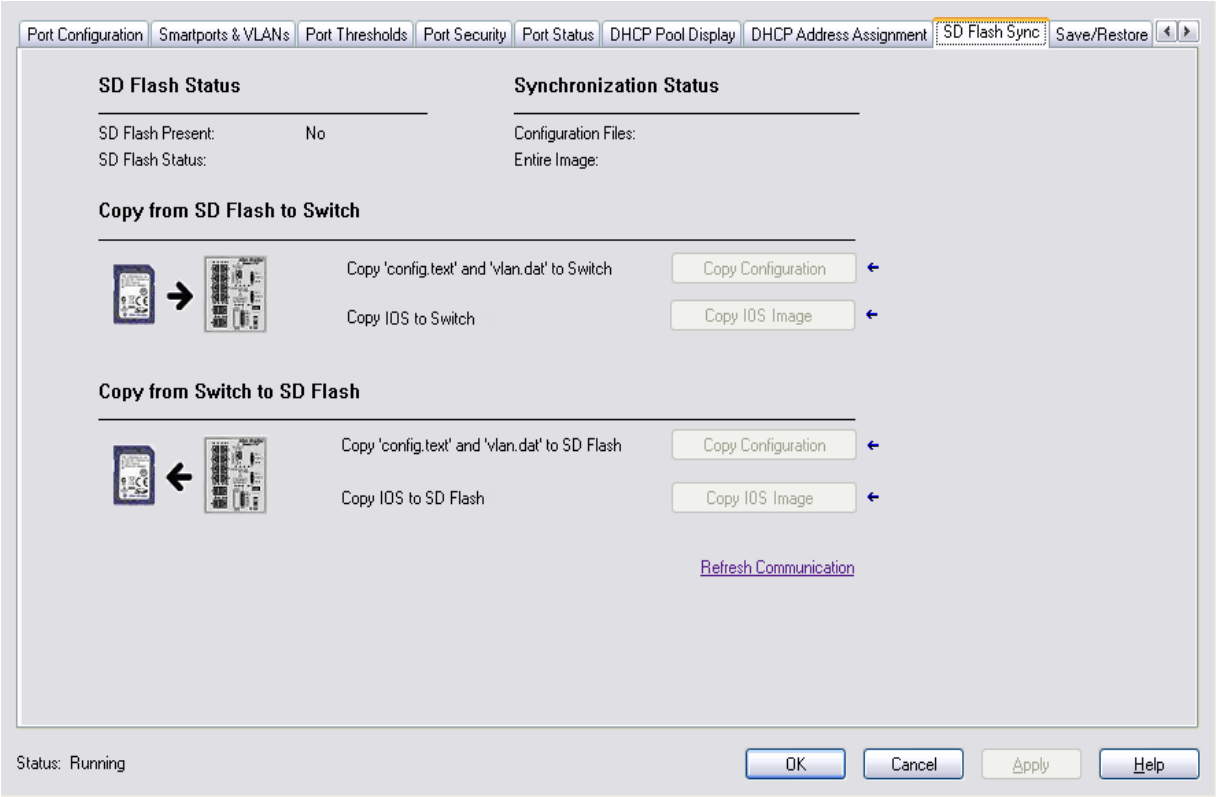


Table 47 - SD Flash Sync Tab Fields

Field	Description
SD Flash Status	Indicates whether the SD card is present and the card's status.
Synchronization Status	Indicates whether the configuration files and the IOS are synchronized or unsynchronized.
Copy from SD Flash to Switch	Choose from these options: • Copy Configuration • Copy IOS Image
Copy from Switch to SD Flash	Choose from these options: • Copy Configuration • Copy IOS Image

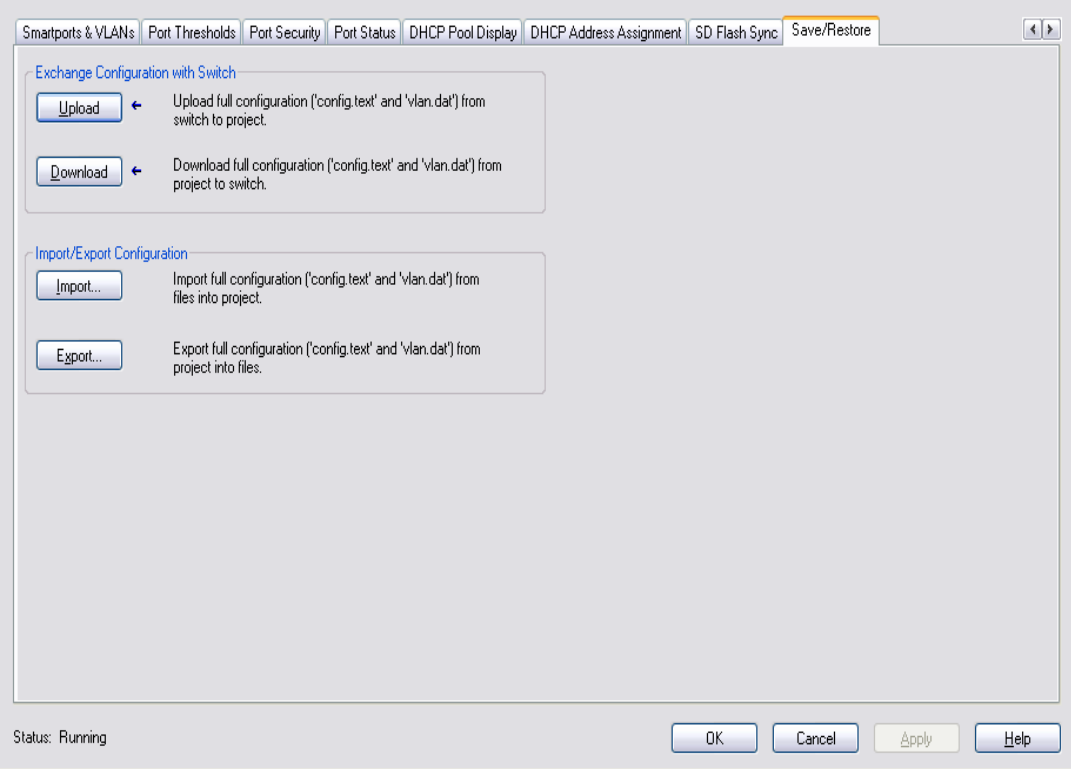
Save and Restore the Switch Configuration

Use this tab to do the following:

- Save the switch configuration to a file for archiving
- Restore a switch configuration stored locally on the computer or within the Logix Designer application project.

You must be online to save and restore configuration files. Most of the settings appear dimmed when the switch is offline.

Be prepared to enter a valid switch password to save and restore a switch configuration.



The switch configuration consists of these two files:

- Text file containing configuration parameters
- Binary file containing VLAN information

Once the switch configuration is uploaded to the project file in the Logix Designer application, the switch configuration can be exported as computer files by using the Export button.

You can import a switch configuration from the appropriate files on your computer to the project by using the Import button on the switch AOP. You can then download the configuration to the switch by using the Download button on the AOP. Refer to Save and Restore the Switch Configuration on page 234 for more information on the Save and Restore feature.

Troubleshoot the Switch

Topic	Page
Verify Boot Fast	235
IP Address Issues	235
Device Manager Web Interface Issues	236
Switch Performance	237
Access Direct Managed Mode	237
Restart or Reset the Switch	239
Recover the Switch Firmware and Restore Factory Defaults	240
Troubleshoot a Firmware Upgrade	241

This chapter helps you resolve issues related to Stratix 5700 switches, as well as perform common functions such as resetting the switch.

For additional troubleshooting, refer to the following:

- Diagnose Cabling Problems on page 176
- View System Log Messages on page 177

Verify Boot Fast

Boot fast failures are potentially fatal to the switch. Contact your Rockwell Automation representative if your switch does not successfully complete boot fast. You can disable the boot fast and run a power-on self test (POST) by using the CLI.

IP Address Issues

These are some basic troubleshooting tips for issues related to the switch IP address.

Issue	Resolution
IP address is not received from DHCP server	If the switch does not receive an IP address from an upstream device operating as a DHCP server, make sure that the upstream device is operating as a DHCP server and again follow the procedures to set up the switch in Chapter 1, About the Switches .
Switch has wrong IP address	If the switch is installed in your network but you cannot access the switch because it has the wrong IP address, assign a new switch IP address. Refer to Access Direct Managed Mode on page 237 to assign the IP address, and then update the switch IP address on the Device Manager Express Setup window.

Device Manager Web Interface Issues

These are some basic troubleshooting for issues related to displaying the Device Manager Web interface.

Issue	Resolution
Device Manager Web interface does not display	If you cannot display the Device Manager Web interface from your computer or laptop, make sure that you entered the correct switch IP address in the browser. If you entered the correct switch IP address in the browser, make sure that the switch and your computer or laptop are in the same network or subnetwork: • For example, if your switch IP address is 172.20.20.85 and your computer or laptop IP address is 172.20.20.84, both devices are in the same network. • For example, if your switch IP address is 172.20.20.85 and your computer or laptop IP address is 10.0.0.2, the devices are in different networks and cannot directly communicate without a router. You must either change the switch IP address or change the computer or laptop IP address. • If the issue persists, follow the procedure in the Access Direct Managed Mode section on page 237, and then update the switch network settings on the device manager Express Setup window. • If the issue still persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 240.
Device Manager Web interface is not operating properly	If the Device Manager Web interface does not operate properly (for instance, the device manager is not responding), follow the procedure in the Access Direct Managed Mode section on page 237, and then update the switch network settings on the Device Manager Web interface Express Setup window. If the issue persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 240.
Device Manager Web interface is not accessible through the network	If you cannot access the device manager remotely from a Web browser, follow the procedure in the Access Direct Managed Mode section on page 237.

Switch Performance

These are some basic troubleshooting for issues related to switch performance.

Issue	Resolution
Speed, Duplex, and Autonegotiation	If the port statistics show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors, this can indicate a speed or duplex mismatch. A common issue with speed and duplex occurs when the duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a workstation or server. This can happen when manually setting the speed and duplex or from autonegotiation issues between the two devices. A mismatch occurs under these circumstances: • A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port. • A port is set to autonegotiate, and the connected port is set to full-duplex with no autonegotiation. To maximize switch performance and be sure of a link, follow one of these guidelines when changing the settings for duplex and speed: • Let both ports autonegotiate both speed and duplex. • Manually set the same speed and duplex parameters for the ports on both ends of the connection to the same values. • If a remote device does not autonegotiate, configure the duplex settings on the two ports to the same values. The speed parameter can adjust itself even if the connected port does not autonegotiate.
Autonegotiation and network interface cards (NICs)	Issues sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. It is common for devices like laptops or other devices to be set to autonegotiate as well, yet sometimes autonegotiation issues occur. To troubleshoot autonegotiation issues, try manually setting both sides of the connection. If this does not solve the issue, there could be an issue with the firmware or software on your NIC. You can resolve this by upgrading the NIC driver to the latest firmware or software available from the manufacturer.
Cabling distance	If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines.

Access Direct Managed Mode

You can display the Device Manager Web interface and manage the switch through a physical connection between one of the switch ports and your computer or laptop. This type of management connection is referred to as the Direct Managed mode. This mode is typically used to connect to the switch by using the Device Manager Web interface when the IP address of the switch is unknown.

Before you can access Direct Managed mode, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

To access the Direct Managed mode, follow these steps.

1. Press the Express Setup button until the Setup status indicator blinks green and the status indicator of an available switch downlink port blinks green.

   The port with a blinking green status indicator is designated as the Direct Managed mode port. This port is determined by the following:

   - If all downlink ports are not connected to devices or if multiple downlink ports are connected to devices, the first available downlink port is selected as the Direct Managed mode port.
   - If only one downlink port is connected to a device, that port is selected as the Direct Managed mode port.

   If there is no available switch downlink port to which to connect your computer or laptop, disconnect a device from one of the switch downlink ports, and then press the Setup button again until the Setup status indicator and the port status indicator blink green.

2. Use a Category 5 Ethernet cable to connect your computer or laptop to the switch port with the blinking port status indicator.

3. Wait until the port status indicators on the switch and your computer or laptop are solid green.

   The solid green port status indicators means a successful connection between the two devices.

4. Start a Web browser on your computer or laptop.

   A password prompt, followed by the Device Manager Web interface page appears.

   If the Device Manager Web interface does not appear, make sure that any pop-up blockers or proxy settings in your browser software are disabled and that any wireless clients running on your computer or laptop are disabled.

   If the Device Manager Web interface still does not appear, enter a URL in your browser, such as http://www.rockwellautomation.com. The browser redirects to the Device Manager Web interface.

Restart or Reset the Switch

If you cannot solve an issue by reconfiguring a feature, either restarting or resetting the switch can solve the issue or help you to eliminate probable causes. If the issue exists after you reset the switch to its default settings, it is unlikely that the switch is causing the issue.

Option	Description
Restart	This option restarts the switch without turning off power. The switch retains its saved configuration settings during the restart process. However, the Device Manager Web interface is unavailable during the process. When the process completes, the switch displays the Device Manager Web interface. **IMPORTANT:** Restarting the switch interrupts connectivity of your devices to the network.
Reset the Switch to Factory Defaults	This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch. **ATTENTION:** Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to the factory default settings. The same software image is retained. You need to reconfigure the basic switch settings. Refer to ArmorStratix 5700 Switch Installation on page 57. **ATTENTION:** Resetting the switch interrupts connectivity of your devices to the network.

IMPORTANT Restarting or resetting the switch interrupts connectivity of your devices to the network.

Restart the Switch from the Device Manager Web Interface

From the Device Manager Web interface, on the Restart/Reset dialog box, click Restart the Switch.

This option restarts the switch without turning off power. The Device Manager Web interface is unavailable during the restart process. When the process completes, the switch displays the Device Manager Web interface.

If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode section on page 237 to access Direct Managed mode.

Restart the Switch from the Logix Designer Application

From Module Properties dialog box within the Logix Designer application, do the following.

1. Click the Module Info tab.
2. Click Reset Module.

   A password prompt appears.
3. Enter your password and click Enter.

Reset the Switch to Factory Defaults

ATTENTION: Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to its factory default. The same software image is retained. To manage the switch or to display the device manager, you need to reconfigure the basic switch settings (as described in Chapter 4, Manage the Switch via the Device Manager Web Interface) and use the new IP address.

IMPORTANT Restarting the switch interrupts connectivity of your devices to the network.

From the Device Manager Web interface, do the following.

1. Access the Device Manager Web interface Restart/Reset dialog box.
2. Click Reset the Switch.

   This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch.

   If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode section on page 237 to access Direct Managed mode. Then go back to step 1, above.

Recover the Switch Firmware and Restore Factory Defaults

Before you can recover switch firmware, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

If the image is corrupted, you can recover the switch firmware. A symptom of corrupted firmware is the switch continuously trying to restart.

Other reasons to recover the switch firmware are if you deleted the image due to a failed firmware upgrade and if you have forgotten the switch password.

Recovering the switch firmware involves deleting all switch configuration settings and returning the switch to its factory default settings. To return the switch to its factory default settings, follow these steps.

1. With the switch already powered up and started, press and hold the Express Setup button until the Setup and EIP Net status indicators turn red.

   This process takes approximately 18...20 seconds.
2. Release the Express Setup pushbutton.

3. Wait for the switch to restart.

   The Express Setup indicator begins flashing when the switch has completed restarting. The switch has now been returned to factory defaults.

4. Set up the switch, as described in ArmorStratix 5700 Switch Installation on page 57.

5. Refer to Troubleshoot a Firmware Upgrade on page 241 and follow the procedure to upgrade the firmware.

Troubleshoot a Firmware Upgrade

If you attempted to upgrade the switch firmware but received a message that the upgrade failed, make sure that you still have access to the switch. If you still have switch access, follow these steps.

1. Make sure that you downloaded the correct .tar file from http://www.rockwellautomation.com.

2. If you downloaded the correct .tar file, refresh your Device Manager Web interface browser session to make sure that there is connectivity between the switch and your computer or laptop or network drive.
   - If you have connectivity to the switch and the Device Manager Web interface, retry the upgrade.
   - If you do not have connectivity to the switch and the Device Manager Web interface, refer to Recover the Switch Firmware and Restore Factory Defaults on page 240.

Notes:

Module-defined Data Types

Topic	Page
Module-defined Input Data Type (6-port Gb switches)	245
Module-defined Output Data Type (6-port Gb switches)	246
Module-defined Input Data Type (6-port switches)	246
Module-defined Output Data Type (6-port switches)	247
Module-defined Input Data Type (8-port switches)	247
Module-defined Output Data Type (8-port switches)	248
Module-defined Input Data Type (10-port Gb switches)	249
Module-defined Output Data Type (10-port Gb switches)	250
Module-defined Input Data Type (10-port switches)	250
Module-defined Output Data Type (10-port switches)	252
Module-defined Input Data Type (16-port switches)	252
Module-defined Output Data Type (16-port switches)	254
Module-defined Input Data Type (18-port Gb switches)	257
Module-defined Output Data Type (18-port Gb switches)	260
Module-defined Output Data Type (20-port Gb switches)	263
Module-defined Input Data Type (20-port switches)	264
Module-defined Output Data Type (20-port switches)	266
Module-defined Input Data Type (24-port switches)	267
Module-defined Output Data Type (24-port switches)	270

In the Logix Designer application, predefined tags for Input and Output data types have a structure corresponding to the switch selected when it was added to the I/O tree. Its members are named in accordance with the port names.

You can disable a switch port by setting the corresponding bit in the output tag. The output bits are applied every time the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied.

The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using the Device Manager Web interface or the CLI, the port setting can be overridden by the output bits the next time they are applied. The output bits always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.

The tables in this appendix list module-defined data types for Stratix 5700 switches. The tables include information for input (as indicated by an I) and output (as indicated by an O).

Module-defined Input Data Type (6-port Gb switches)

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_1Connected	BOOL	Decimal	LinkStatus:5
PortGi1_2Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (6-port Gb switches)

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_1Disable	BOOL	Decimal	DisablePort:5
PortGi1_2Disable	BOOL	Decimal	DisablePort:6

Module-defined Input Data Type (6-port switches)

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (6-port switches)

AB:STRATIX_5700_6PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6

Module-defined Input Data Type (8-port switches)

AB:STRATIX_5700_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:5
PortFa1_8Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7

AB:STRATIX_5700_8PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (8-port switches)

AB:STRATIX_5700_8PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8

Module-defined Input Data Type (10-port Gb switches)

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_1Connected	BOOL	Decimal	LinkStatus:9
PortGi1_2Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (10-port Gb switches)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_1Disable	BOOL	Decimal	DisablePort:9
PortGi1_2Disable	BOOL	Decimal	DisablePort:10

Module-defined Input Data Type (10-port switches)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (10-port switches)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10

Module-defined Input Data Type (16-port switches)

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	

AB:STRATIX_5700_16PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (16-port switches)

AB:STRATIX_5700_16PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16

Module-defined Input Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Input Data Type (18-port Gb switches)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (18-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

Module-defined Input Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (20-port Gb switches)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

Module-defined Input Data Type (20-port switches)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	
PortFa1_20Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (20-port switches)

AB:STRATIX_5700_20PORT_MANAGED:O:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20

Module-defined Input Data Type (24-port switches)

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
Fault	DINT	Binary	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
PortFa1_21Connected	BOOL	Decimal	LinkStatus:21
PortFa1_22Connected	BOOL	Decimal	LinkStatus:22
PortFa1_23Connected	BOOL	Decimal	LinkStatus:23
PortFa1_24Connected	BOOL	Decimal	LinkStatus:24
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
PortFa1_21UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:21
PortFa1_22UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:22
PortFa1_23UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:23
PortFa1_24UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:24
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
PortFa1_21Threshold	BOOL	Decimal	ThresholdExceeded:21
PortFa1_22Threshold	BOOL	Decimal	ThresholdExceeded:22
PortFa1_23Threshold	BOOL	Decimal	ThresholdExceeded:23
PortFa1_24Threshold	BOOL	Decimal	ThresholdExceeded:24
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	

AB:STRATIX_5700_24PORT_MANAGED:I:0			
Member Name	**Type**	**Default Display Style**	**Valid Values**
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	
PortFa1_20Utilization	SINT	Decimal	
PortFa1_21Utilization	SINT	Decimal	
PortFa1_22Utilization	SINT	Decimal	
PortFa1_23Utilization	SINT	Decimal	
PortFa1_24Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binary	

Module-defined Output Data Type (24-port switches)

AB:STRATIX_5700_24PORT_MANAGED:0:0

Member Name	Type	Default Display Style	Valid Values
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20
PortFa1_21Disable	BOOL	Decimal	DisablePort:21
PortFa1_22Disable	BOOL	Decimal	DisablePort:22
PortFa1_23Disable	BOOL	Decimal	DisablePort:23
PortFa1_24Disable	BOOL	Decimal	DisablePort:24

Port Assignments for CIP Data

This table identifies the instance numbers of the Ethernet link object associated with each port on the switch. Instance 0 does not apply to all the ports as it does for bit maps.

The bit numbers identify each port when they are contained in a structure of all the ports, such as in the output assembly. Bit 0 refers to any or all ports.

Instance/Bit	6-port Switch	6-port Gb Switch	8-port Switch	10-port Switch	10-port Gb Switch	16-port Switch	18-port Gb Switch	20-port Switch	20-port Gb Switch	24-port Switch
Bit 0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
Instance/Bit 1	Fa1/1	Fa/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Instance/Bit 2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Instance/Bit 3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Instance/Bit 4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Instance/Bit 5	Fa1/5	Gi1/1	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5
Instance/Bit 6	Fa1/6	Gi1/2	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6
Instance/Bit 7			Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7
Instance/Bit 8			Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8
Instance/Bit 9				Fa1/9	Gi1/1	Fa1/9	Fa1/9	Fa1/9	Fa1/9	Fa1/9
Instance/Bit 10				Fa1/10	Gi1/2	Fa1/10	Fa1/10	Fa1/10	Fa1/10	Fa1/10
Instance/Bit 11						Fa1/11	Fa1/11	Fa1/11	Fa1/11	Fa1/11
Instance/Bit 12						Fa1/12	Fa1/12	Fa1/12	Fa1/12	Fa1/12
Instance/Bit 13						Fa1/13	Fa1/13	Fa1/13	Fa1/13	Fa1/13
Instance/Bit 14						Fa1/14	Fa1/14	Fa1/14	Fa1/14	Fa1/14
Instance/Bit 15						Fa1/15	Fa1/15	Fa1/15	Fa1/15	Fa1/15
Instance/Bit 16						Fa1/16	Fa1/16	Fa1/16	Fa1/16	Fa1/16
Instance/Bit 17								Fa1/17	Fa1/17	Fa1/17
Instance/Bit 18								Fa1/18	Fa1/18	Fa1/18
Instance/Bit 19							Gi1/1	Fa1/19	Gi1/1	Fa1/19
Instance/Bit 20							Gi1/2	Fa1/20	Gi1/2	Fa1/20
Instance/Bit 21										Fa1/21
Instance/Bit 22										Fa1/22
Instance/Bit 23										Fa1/23
Instance/Bit 24										Fa1/24
Instance/Bit 27	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1

Notes:

Cables and Connectors

Topic	Page
10/100 and 10/100/1000 Ports	273
Dual-purpose Ports (combo ports)	276
Console Ports	277
Alarm Ports	279
Cable and Adapter Specifications	280
Adapter Pinouts	280

For recommended cables, refer to the Stratix Ethernet Device Specifications Technical Data, publication 1783-TD001.

10/100 and 10/100/1000 Ports

The 10/100 and 10/100/1000 Ethernet ports on switches use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

TIP The auto-MDIX feature is enabled by default.

Figure 10 - 10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

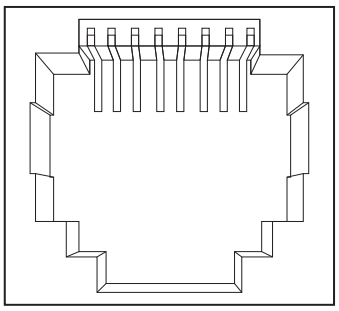
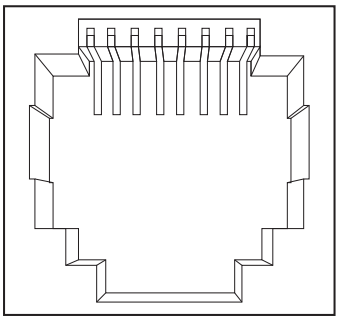
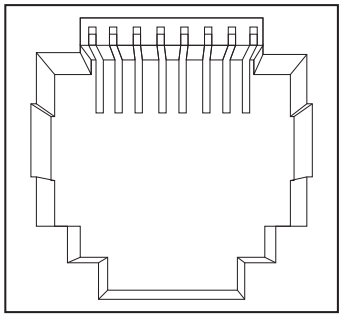


Figure 11 - 10/100/1000 Connector Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

PoE ports integrate power and data signals on the same wires. The ports use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

Figure 12 - 10/100 PoE Connector Pinouts and Power Sourcing Equipment (PSE) Voltage

Pin	Label	Alternative A (MDI)	1 2 3 4 5 6 7 8
1	RD+	Positive V PSE	
2	RD-	Positive V PSE	
3	TD+	Negative V PSE	
4	NC		
5	NC		
6	TD-	Negative V PSE	
7	NC		
8	NC		

Connect to 10BASE-T- and 100BASE-TX-Compatible Devices

The auto-MDIX feature is enabled by default. Follow the cabling guidelines below when the auto-MDIX feature has been disabled.

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers, workstations, and routers, you can use a two or four twisted-pair, straight-through cable wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The wire connected to the pin on the outside of the left plug must be a different color from the wire connected to the pin on the inside of the right plug.

The following figures show these schematics:

- Two twisted-pair, straight-through cable
- Four twisted-pair, straight-through cable

Figure 13 - Two Twisted-pair Straight-through Cable Schematic

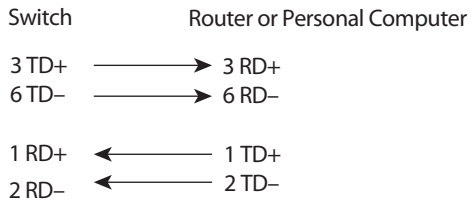
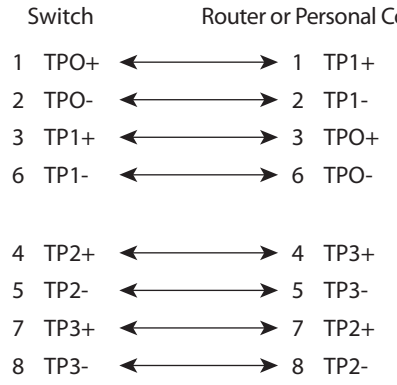


Figure 14 - Four Twisted-pair Straight-through Cable Schematic



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

The following figures show these schematics:

- Two twisted-pair, crossover cable schematics
- Four twisted-pair, crossover cable schematics

Use a straight-through cable to connect two ports when only one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device or PoE port.

Figure 15 - Two Twisted-pair Crossover Cable Schematic

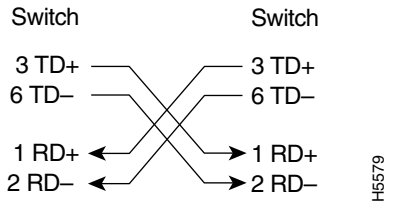
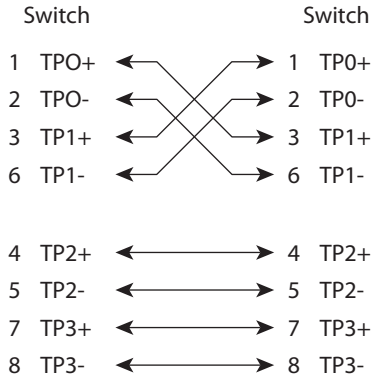


Figure 16 - Four Twisted-pair Crossover Cable Schematic

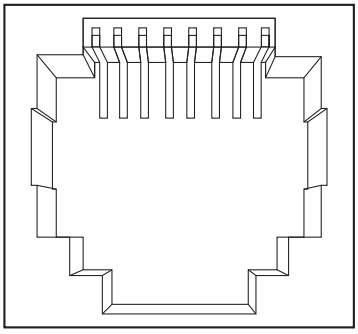


Dual-purpose Ports (combo ports)

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Figure 17 - Ethernet Port RJ45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports.

IMPORTANT The auto-MDIX feature is enabled by default. For configuration information for this feature, see the switch software configuration guide or the switch command reference.

Console Ports

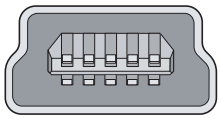
Console ports enable you to connect a switch to a computer if you use the Command-line interface (CLI) to configure and monitor a switch.

Stratix 5700 Console Ports

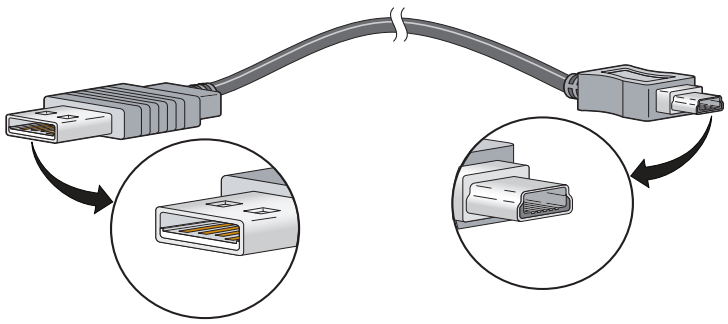
Stratix 5700 switches have two console ports:

- A USB 5-pin mini-Type B port on the front panel
- An RJ45 console port on the rear panel

Only one console port can be active at one time.



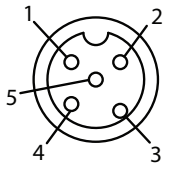
The USB console port uses a USB Type A to 5-pin mini-Type B cable. The USB Type A-to-USB mini-Type B cable is not supplied.



ArmorStratix 5700 Console Port

ArmorStratix 5700 switches have one console port. The console port uses a male 5-pin DC Micro-style (M12) connector configuration cordset, such as Allen-Bradley Bulletin 889D. For more information, see publication 889DS-PP001.

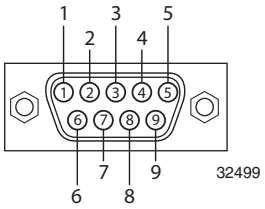
Figure 18 - Console Port Pinout



1. RTS
2. CTS
3. TXD
4. RXD
5. GND

32500

Figure 19 - DB9 Connector Pinout



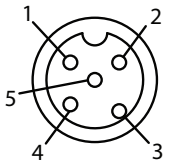
32499

M8 Cable		DB9-S Connector	
Pin	**Function**	**Pin**	**Function**
1	RTS	8	CTS
2	CTS	7	RTS
3	TD	2	RD
4	RD	3	TD
5	GRND	5	GRND

Alarm Ports

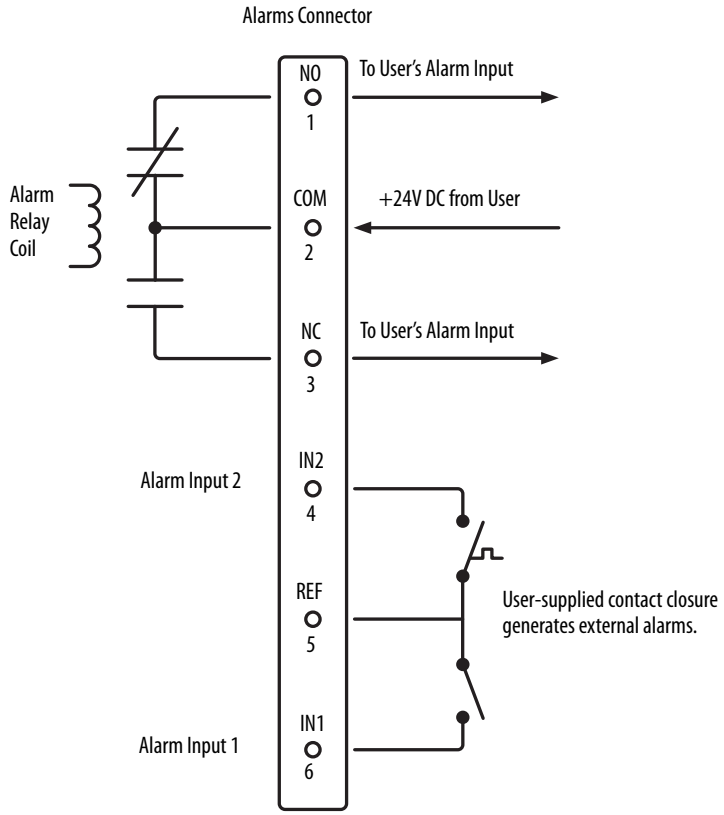
The front-panel alarm relay connector and ports are described below. The alarm connector uses a male 5-pin DC Micro-style (M12) connector configuration cordset, such as Allen-Bradley Bulletin 889D. For more information, see publication 889DS-PP001.

Figure 20 - Alarm Connector Pinout



1. NO
2. NC
3. Unconnected
4. Unconnected
5. Common

Figure 21 - Wiring Example for Alarm Inputs and Outputs



Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

Cable and Adapter Specifications

These sections describe the cables and adapters used with the switches.

SFP Module Cable Specifications

The following lists the cable specifications for the rugged fiber-optic SFP module connections. Each port must match the wave-length specifications on the other end of the cable, and for reliable communication, the cable must not exceed the rated maximum cable length.

Table 48 - Fiber-optic SFP Module Port Cabling Specifications

SFP Module Type	Cat. No.	Wavelength (nm)	Fiber Type	Core Size/Cladding Size (micron)	Modal Bandwidth (MHz/km)(1)	Cable Distance
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62.5/125	500 500	2 km (6562 ft) 2 km (6562 ft)
100BASE-LX	1783-SFP100LX	1310	SMF	G.652[2]	—	10 km (32,810 ft)
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125 62.5/125 50/125 50/125	160 200 400 500	220 m (722 ft) 275 m (902 ft)) 500 m (1640 ft) 550 m (1804 ft)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652[2]	—	10 km (32,810 ft)

(1) Modal bandwidth applies only to multi-mode fiber.

PoE Port Cable Specifications

For PoE ports, use a Category 5 (Cat 5) cable with a distance of up to 100 m (328 ft).

Adapter Pinouts

The following table lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Table 49 - Pinouts with DB-9 Pin

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device. The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

Table 50 - Pinouts with DB-25 Pin

Switch Console Port (DTE)	RJ45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Notes:

History of Changes

Topic	Page
1783-UM004D-EN-P, March 2014	283
1783-UM004C-EN-P, December 2013	283
1783-UM004B-EN-P, June 2013	285

This appendix summarizes the revisions to this manual. Reference this appendix if you need information to determine what changes have been made across multiple revisions. This can be especially useful if you are deciding to upgrade your hardware or software based on information added with previous revisions of this manual.

1783-UM004D-EN-P, March 2014

Change
Updated Device Manager hardware and software requirements
New Express Setup window
New process for enabling routing
New DeviceManager Web interface

1783-UM004C-EN-P, December 2013

Change
Access product release notes
Description of switches with Power over Ethernet (PoE)
PoE switch dimensions
PoE port descriptions
AWG wire size for connecting external grounding screw
Wire the PoE power source
Attach the Poe power connector
Connect to PoE Ports
Express setup and SD card
Port numbering on switches with PoE

PoE feature descriptions
Configure PoE via the Device Manager Web interface
PoE port connector pinouts and cable specifications

1783-UM004B-EN-P, June 2013

Change
Studio 5000 Logix Designer™ application is the rebranding of RSLogix 5000 software
Description of 1783-BMS10CGN and 1783-BMS20CGN switches
Network address translation (NAT) software feature
Port numbering for 1783-BMS10CGN and 1783-BMS20CGN switches
Overview of NAT
Configure NAT via the Device Manager Web interface
Monitor NAT statistics via the Device Manager Web interface
Configure NAT via the Logix Designer application
Monitor NAT diagnostics via the Logix Designer application

Numerics

10/100 ports
cable lengths 32, 58
connecting to 52, 66
10/100/1000 ports
cable lengths 32, 58
connecting to 52, 66

A

adapter pinouts
terminal
RJ45-to-DB-25 281
RJ45-to-DB-9 280
address aliasing 93
address translation 101
airflow, required clearance 31, 58
alarm relay connections
connection procedures 50, 51, 65
alert log 177
allocation, memory 57, 67
announce interval 147
announce receipt timeout interval 147
ArmorStratix switches
catalog number descriptions 16
dimensions 21
installation 57-66
assign VLANs to NAT instance 105
Auto mode, PoE 87
auto-MDIX 53, 273, 276
default 133
setting 133
autonegotiation
Duplex mode 133
speed 133
troubleshoot 237

B

Boundary mode 145
timing message settings 146
broadcast storms 95

C

cable diagnostics 207, 209
cables
connect to PoE ports 54, 66
crossover
four twisted-pair pinout, 1000BASE-T ports 276
identifying 274
using 275
optical 280
SFP module 280
straight-through
two twisted-pair pinout 275
using 274
cabling
10/100/1000 ports 52, 66
auto-MDIX 53, 273, 276
CIP data 190
CIP network connections 188
CIP Sync time synchronization 100
clearance 32, 58
clock
parent 145
synchronization 145
connecting
to 10/100/1000 ports 52, 66
to DC power 35, 40, 60, 64
to external alarm devices 49, 51, 65
to SFP modules 55
connection
Direct Managed mode 237
properties 195
connectors and cables
10/100/1000 274, 275
console 281
dual-purpose 276
console port
specifications 281
crossover cable
pinout
four twisted-pair, 1000BASE-T ports 276
cryptographic software
SSL 111
customization
DHCP persistence 139
DHCP server 137
IP address
DHCP IP address pool 138, 139
switch port 141
IP address (for connected devices) 137, 139
IP address (switch port) 139
Smartport roles 83

D

DC power, connecting to 35, 40, 60, 64
default gateway
NAT 101, 156, 220
default router 139
default VLAN 90, 126
delay request interval 147
denial-of-service attack 95
Device Manager
access Web interface 118
hardware requirements 26
overview 26
software requirements 26
troubleshoot 236

DHCP
address assignment 212
IP address pool 138
persistence 139
pool display 210
server 100
troubleshoot 235
Direct Managed mode 237
DNS server1 and 2 139
domain name 139
dual-purpose ports
connectors and cables 276
duplex
troubleshooting 237
Duplex mode
default 133
setting 133

E

electrical noise, avoiding 32, 58
electrostatic discharge 36, 57
End-to-end Transparent mode 145
EtherChannels
creating 135
deleting 135
modifying 135
EtherNet/IP protocol 83, 174, 204

F

firmware upgrade, troubleshoot 241
front panel
clearance 32, 58
Full-duplex mode 133
functional ground lug warning 39, 62

G

grounding procedures 38, 40, 62, 63

H

Half-duplex mode 133
hardware features 22
hardware requirements
Device Manager Web interface 26

I

IEEE power classifications 86
IGMP snooping
and address aliasing 93
definition 93
features 164
Initial Setup mode 178
installation
attach the power and relay connector 43, 52
DIN rail 37
grounding procedures 38, 40, 62, 63
mount ArmorStratix switch 61
POST 35, 60
pre-installation information and guidelines 32, 58
required clearance 31, 58
verify switch operation 34, 60
verifying switch operation 35, 60
wiring the relays 49, 51, 65
IP address
customization
DHCP IP address pool 138, 139
switch port 141
customization (connected devices) 137
customization (switch port) 139
DHCP IP address pool
ending range 139
starting range 138
Express Setup 142
switch port 141
assigning 141
deleting 141
modifying 141
translation 101
troubleshoot 235
DHCP 235
wrong IP address 235

L

lease length 139
link integrity, verify with REP 110
Logix Designer application 11, 187

M

management interface 26
NAT 105
management VLAN 90
memory 57, 67
MIBs, supported 112
mismatch prevention, Smartport roles 84
modes, management
Direct Managed 237
Initial Setup 178
module information 196
module properties 192
module-defined data types 244
monitoring
alert log 177
network analyzer 113
port mirroring 113
multicast storm 95

N

NAT
configuration considerations 106
configuration overview 101
configure via Device Manager Web interface 153-162
configure via Logix Designer application 215-228
definition 101
diagnostics 172, 229-232
management interface 105
traffic permits and fixups 106, 161, 228
translation entry types 104
network address translation. ***See*** **NAT**
noise, electrical 32, 58

O

Overview tab, dashboard 171

P

parent clock 145
pinouts
crossover cables
four twisted-pair, 1000BASE-T ports 276
PoE 274
RJ45-to-DB-25 terminal adapter 281
RJ45-to-DB-9
terminal adapter 280
straight-through cables
two twisted-pair 275
PoE
configure via Device Manager Web interface 142
configure via Studio 5000 environment 201
features 85-89
initial power allocation 86
pinouts 274
power management modes 87
powered device detection 86
wire DC power source 45
pool name 141
pop-up blockers 26, 238
port
assignments for CIP data 271
configuration 200
connection procedures 66
diagnostics 208
dual-purpose 56
numbering 133
roles 125
security 97, 162, 206
status 207
threshold 134
thresholds 205
type 152
port settings
auto-MDIX 133
description 133
descriptions of 132
Duplex mode 133
enable/disable 133
default 133
speed 133
default 133
POST
description 35, 60
results 35, 60
power 35, 60
connecting to
DC 40
DC power 64
power and relay connector
connecting to the switch 43, 52
power classifications 86
Precision Time Protocol 164
See also PTP 145
prevent electrostatic discharge 36, 57
proxy settings 26, 238
PTP 164
Boundary mode 145
timing message settings 146
Synchronization Clock mode 145
PTP End-to-end Transparent mode 145
PTP, Precision Time Protocol 100

R

rear panel, clearance 32, 58
Receive Detail tab, dashboard 171
recovery
firmware upgrade 241
switch software 240
redundancy
EtherChannel 99
relays
wiring 51
removing SFP modules 48
REP 107
open segment 108
ring segment 109
segments
characteristics 109
verify link integrity 110
REP Admin VLAN 152
REP segments 107
configure 151
reset, troubleshoot 240
residence time 145
Resilient Ethernet Protocol
see REP 107
roles 105
RSLinx software 189
RSTP
features 149
RSWho 189

S

save and restore 234
SD card
- install or remove 33, 59
- synchronize
  - configuration 184
- synchronize IOS files 184

SD Flash Sync 233
SDM template 181
security
- configure for ports 162
- violations 98

segment ID 152
segment topology change notices
- See also STCNs 152

SFP modules
- bale-clasp latch removal 48
- cables 280
- connecting to 55

Smartport roles
- applying 125
- changing VLAN memberships 126
- customization 126
  - optimize ports 83
- mismatch prevention 84

Smartport roles and NAT 105
Smartport roles and VLANs 203
SNMP
- configuring 165
- default 165
- MIBs supported 112

snooping, IGMP 93
software features
- customization
  - DHCP persistence settings 139
  - DHCP server settings 137
  - Smartport roles 83
- troubleshoot
  - firmware upgrade 183

software requirements
- Device Manager 26

Spanning Tree Protocol 107
- See also Rapid Spanning Tree Protocol

specifications 13
speed
- setting 133
- troubleshoot 237

Static mode, PoE 88
status indicators 119
STCN interface 152
STCN segment 152
STCN STP 152
storm control
- described 95
- thresholds 95

straight-through cable
- pinout
  - two twisted-pair 10/100 ports 275, 276

Studio 5000 environment 11, 187
subnet mask
- DHCP IP address pool 138

subnet translation 104, 156, 159, 161, 219, 223
switch
- manage via Device Manager 26
- monitoring
  - alert log 177
  - network analyzer 113
  - port mirroring 113
- status 199
- troubleshoot 235
  - Device Manager display 236
  - Device Manager not accessible 236
  - Device Manager problems 236
  - DHCP 235
  - Direct Managed mode 237
  - firmware upgrade 241
  - IP address problems 235
  - reset switch 240
  - switch software 240
  - wrong IP address 235

switch configuration
- properties 197
- save and restore 234

switch software, troubleshoot 240
switch, power-on 35, 60
sync interval 147
sync limit 147
Synchronization Clock mode
- Boundary 145, 146
- End-to-end Transparent 145
- setting 145

T

threshold
- port 134
- traffic level 95

timing message settings, PTP Boundary mode 146
traffic fixups and NAT 106, 161, 228
traffic permits and NAT 106, 161, 228
traffic suppression 95
translate IP addresses 101
translation entry types 104
Transmit Detail tab, dashboard 171
troubleshoot
- Device Manager display 236
- Device Manager not accessible 236
- Device Manager problems 236
- DHCP 235
- Direct Managed mode 237
- firmware upgrade 183, 241
- IP address problems 235
- reset switch 240
- speed, duplex, and autonegotiation 237
- switch 235
- switch performance 237
- switch software 240
- wrong IP address 235

U

unicast storm 95
upgrade firmware 183

V

verify switch operation 34, 60
verifying switch operation 35, 60
View list 121
VLAN memberships
changing 126
prerequisite 126
VLANs
assign to NAT instance 105, 154, 157, 217, 221
default VLAN 90
grouping different users 92
isolate traffic 92
management VLAN 90

W

warnings
functional ground lug 62
WINS server1 and 2 139

Notes:

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Automation maintains current product environmental information on its website at http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM004E-EN-P - June 2014
Supersedes Publication 1783-UM004D-EN-P - March 2014

Copyright © 2014 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.